TRANSMITTAL SLIP / NOTE D'ENVOI

17.05.16

To / À Director		Classification ~~UNCLAS~~ Secret (w/enclosure)
From / De ADP		File / Dossier 900-6-1 (HoC Committees)
Drafting officer / .		Date 2017 05 09

Subject / Sujet

Director's Appearance at SECU: Main Estimates and Supplementary Estimates (C)

Action / Donnez suite	Priority / Priorité	Deadline / Délai
☐ Signature ☐ Comments / Commentaires X Approval / Approbation ☐ Information	☐ Routine X Urgent ☐ Immediate / Immédiate	CSIS / SCRS MAY 11 2017 27009 **1 p.m. 2017 05 10 to ADP** **COB 2017 05 10 to DIR**

Record of Consultation/Approval Rapport de consultation/d'approbation	Consulted Consulter	Concur D'accord Yes Oui	Concur D'accord No Non	Comments / Commentaires
Public Media Liaison	X	(11 05 17)		Please find enclosed a briefing binder in support of your appearance at the House of Commons Standing Committee on Public Safety and National Security (SECU) on 2017 05 15 from 3:30-5:30pm (Location TBC). The Minister will appear for the first hour, with you and other portfolio officials. A list of these officials is enclosed. You and the other representatives will remain at the table to answer questions for the second hour. No opening remarks are required. Please note that requested briefing material on foreign interference has been incorporated as a hot issue card. Further, a summary of the recently released SECU report and relevant press conference are included as supporting documents. Public Media Liaison, was also consulted regarding the Hot Issues cards.
DG May 10 '17	X	X		

CSIS / SCRS
MAY 10 2017
2064
Policy & Foreign Relations

CSIS / SCRS
27009
MAY 10 2017
ADP / DAP

SECU ON MAY 15, 2017
MAIN ESTIMATES AND SUPPLEMENTARY ESTIMATES (A)

WITNESS LIST

FIRST HOUR – 3:30 – 4:30 p.m.

Appearing:	**The Honourable Ralph Goodale, Minister of Public Safety and Emergency Preparedness**

Officials at the Table	**Public Safety**	Malcolm Brown, Deputy Minister
	RCMP	Bob Paulson, Commissioner
	CSIS	Michel Coulombe, Director
	CBSA	John Ossowski, President
	CSC	Don Head, Commissioner
	PBC	Harvey Cenaiko, Chairperson
Official(s) in the Audience	**CMB**	Caroline Weber, ADM

SECOND HOUR – 4:30 – 5:30 p.m.

Officials at the Table	**Public Safety**	Malcolm Brown, Deputy Minister
	RCMP	Bob Paulson, Commissioner
	CSIS	Michel Coulombe, Director
	CBSA	John Ossowski, President
	CSC	Don Head, Commissioner
	PBC	Harvey Cenaiko, Chairperson
Official(s) in the Audience	**CMB**	Caroline Weber, ADM

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

THANKING SECU MEMBERS

ISSUE: The Director of CSIS will be making his final SECU appearance Monday, May 15th. Since the announcement of the new DIR, we have received three Media interview requests: Radio Canada and CBC News, and Vice to interview the DIR for his perspective on the current threat environment Canada is facing as he leaves his post.
Director may wish to thank members of the SECU committee at this time.

FRENCH

- Merci, monsieur le président, de m'avoir invité à comparaître devant vous aujourd'hui. Si vous le permettez, j'aimerais profiter de l'occasion pour remercier les membres du Comité permanent de la sécurité publique et nationale des efforts consacrés sans relâche au cours des dernières années à des enjeux de la plus haute importance pour la sécurité de notre pays.

- Grâce à vous, d'importantes discussions ont été tenues sur la sécurité nationale et la menace terroriste mondiale à laquelle nous faisons face.

- Vous avez aidé les Canadiens à comprendre que le SCRS n'est pas une organisation secrète, mais un organisme astreint au secret. S'il nous a été difficile de fournir des détails parfois, nous avons aussi eu des occasions d'expliquer aux Canadiens, sur cette tribune, les principaux défis que nous avons à relever à l'heure actuelle.

- Au moment où je me prépare à quitter cette organisation, je tiens à réitérer à quel point il a été gratifiant de représenter les hommes et les femmes d'exception du SCRS. Leur dévouement à la protection de ce grand pays est hors pair et indéfectible.

ENGLISH

- Thank you Mr. Chair for the invitation to appear before you today. If I may, I wanted to take this opportunity to thank the members of the Standing Committee on Public Safety and National Security for your continued effort over the past years on issues paramount to our country's safety.

- This committee has helped generate important discussions about National Security and the global threat of terrorism we face.

- You've helped show Canadians that CSIS is not a secret organization, but an organization with secrets. While at times it was difficult to elaborate on details, there were still opportunities to explain to Canadians, through this arena, the key elements we are faced with today.

- As I prepare to leave this organization, I must reiterate how gratifying it has been to represent the exceptional women and men of CSIS. Their unparalleled dedication to the protection of this great country is unwavering.

HOUSE OF COMMONS STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY (SECU)

15 May 2017, 4:30 – 5:30 p.m.

TABLE OF CONTENTS

D. ***Cyber Security***
- NS Framework – Cyber
- TRA and Offensive Cyber Operations
- Cyber Review

E. ***Foreign Cooperation and Information Sharing***
- Establishing Arrangements
- Foreign Cooperation
- Human Rights
- Implementation of Ministerial Direction
- Arrangements with foreign partners

F. ***Security of Canada Information Sharing Act (SCISA)***
- Definitions and Thresholds (SCISA, CSIS Act)
- Safeguards and Accountability
- Implementation
- Experience to date

G. ***National Security Framework***
- CSIS' Role
- CSIS' Cooperation with Domestic Partners
- CSIS' Cooperation with Foreign Partners
- Operational cooperation

H. ***Threat Reduction***
- Implementation
- Number of Measures to Date
- Safeguards
- Cooperation with Partners (RCMP, GAC, CSE)
- Warranted Measures
- Non-Warranted Threat Reduction Activities
- Examples of Warranted Activities

I. ***Lawful Access (Going Dark)***
- Impact of "Going Dark"
- Relationship with CSP
- Data Retention
- Encryption

J. ***Intelligence as Evidence***
- Existing Authorities to Protect Sensitive Information

K. ***Bill C-22: Committee of Parliamentarians***
- Access
- Amendments to Exemptions
- Protection of Classified Information
- Resources
- Relationship with Review Bodies
- Oversight and Review

TAB 4 - **Recent Media Coverage and Trends**

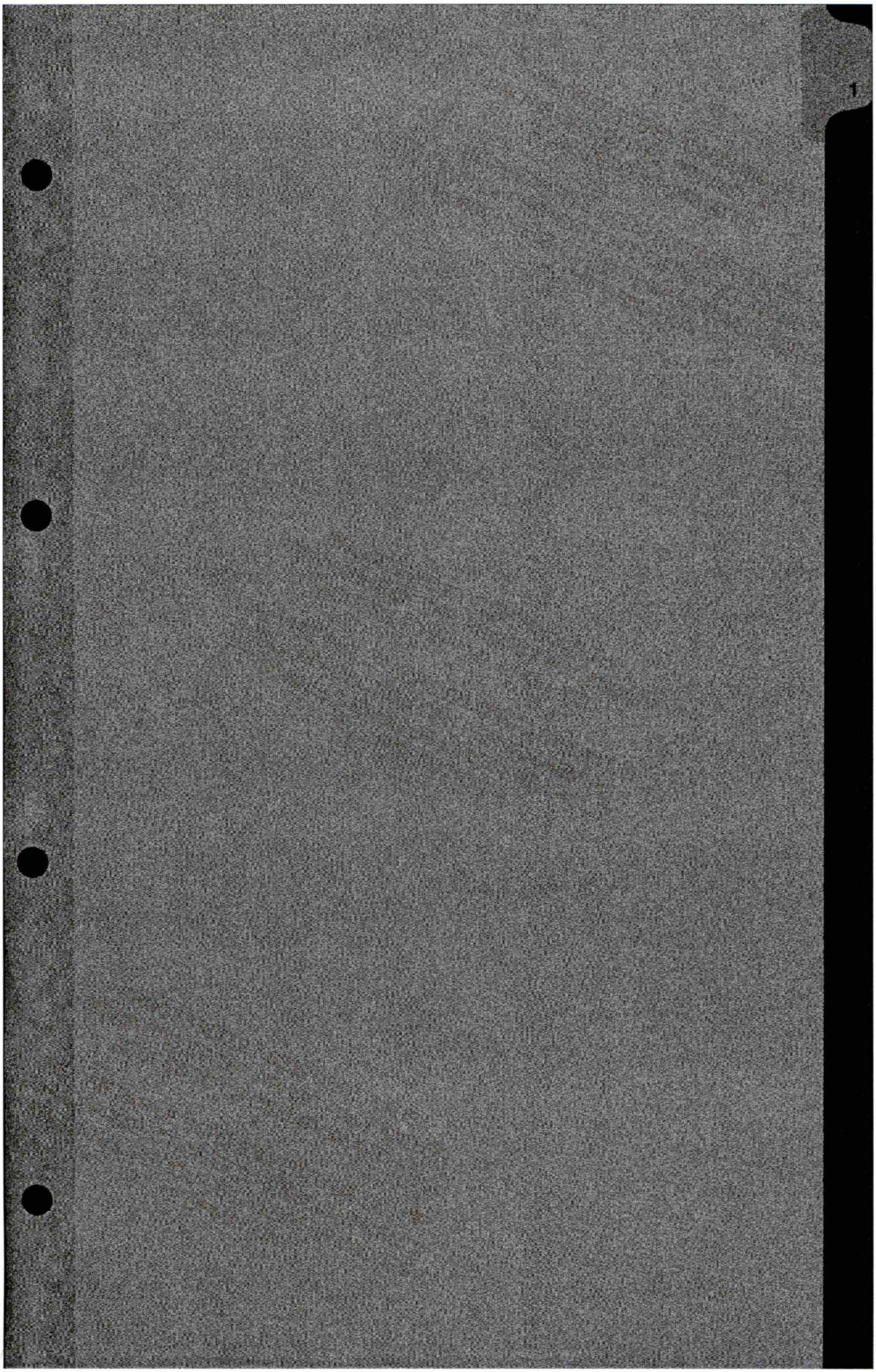
TAB 5 - **Supporting Documents:**

A. ***SECU's Report on the National Security Framework***
- Summary of the Report
- Transcript of Related Press Conference

B. ***Director at SECU, 2016 12 08 (Supps B and Data Retention)***
- Follow-Up on Data Retention

C. ***Director at SECU, 2016 10 06 (NS Framework)***
- Follow-Up on SCISA
- Follow-Up on TRA Examples

TAB 6 - **SECU Membership** (Updated in February 2017)


1

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

A

Date: May 15. 2017
Classification: UNCLASSIFIED
Branch / Agency: CSIS

Question Period Note / Note pour la Période des questions

2017-2018 MAIN ESTIMATES
Canadian Security Intelligence Service

ISSUE: Tabling of the 2017-2018 Main Estimates in Parliament.

- **CSIS is a key partner in protecting Canadians from threats to the safety and security of this country.**
- **While detailed breakdowns of CSIS expenditures are classified, CSIS will receive $577.1M in the Main Estimates for 2017-2018, which represents a 0.9% increase over the previous year.**
- **This funding will allow CSIS to continue its important work in keeping Canadians safe.**

IF PRESSED ON RESOURCES:

- **Like all government agencies, CSIS operates within the budgets it has been allocated by Parliament and adjusts its priorities in accordance with the security environment.**

2017-2018 MAIN ESTIMATES
Canadian Security Intelligence Service

BACKGROUND:

While detailed breakdowns of CSIS expenditures are classified, CSIS does provide general information about its financial resources through documents such as the Main Estimates, the Supplementary Estimates and the CSIS Public Report. CSIS, like other government departments and agencies, is subject to the scrutiny of the Auditor General and other officers of Parliament.

0.9%

I. Highlights of Main Estimates Elements

- The Canadian Security Intelligence Service is seeking approval in the amount of $577.1M in 2017-2018.
- Of this amount, $526.6M falls under Vote 1 (Program Expenditures) and requires approval by Parliament.
- The remaining $50.5M represents statutory forecasts that do not require additional approval.

II. Summary of Net Annual Change in Main Estimates by Program/Initiative

Increase:

- $8.6M in support of Canada's national security and the safety of Canadians.

Decrease:

- $3.6M due to the Budget 2016 reduction in Professional Services, Advertising and Travel.

III. Summary of Net Annual Change in Main Estimates by Vote

Vote 1: Program Expenditures - $526.6M

- The program expenditures for the 2017-2018 Main Estimates result in a net increase of $8.1M or 1.6% from the 2016-2017 Main Estimates.

Increases totaling $11.7M mainly due to :

- $11.7M in support of Canada's national security and the safety of Canadians.

Decreases totaling $3.6M mainly due to :

- $3.6M due to the Budget 2016 reduction in Professional Services, Advertising and Travel.

Statutory Vote: Contribution to Employee Benefit Plan (EBP) - $50.5M

- The net decrease of $3.1M or 5.8% from the 2016-2017 Main Estimates is due to technical adjustments made by TBS and new funding received by government.

Overall Increase: $5.0M

IV. Transfer Payment Highlights

- N/A

V. Detailed Explanation per Program

- N/A

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

- Salary sum
- Capital project

Date: May 15, 2017
Classification: Unclassified
Branch / Agency: CSIS

Question Period Note / Note pour la Période des questions
Supplementary Estimates (C), 2016-2017 **Canadian Security Intelligence Service**
ISSUE: Tabling of the Supplementary Estimates C, 2016-2017 in Parliament.

- **The Supplementary Estimates (C) items will represent an increase of $21.7M to the CSIS authorities from $593.9M to $615.6M.**

- **While CSIS' increase to Voted Appropriations is this amount does not include $0.4M in Statutory Appropriations related to the Employee Benefit Plans and a transfer from National Defence of $0.1M, which, when added, yields a Supplementary Estimates (C) total amount of**

IF PRESSED ON FUNDING TO ADDRESS THE CRISES IN IRAQ AND SYRIA:

- **CSIS is a key partner in efforts to protect Canadians from threats to the safety and security of this country, including the Government's commitments to the Global Coalition against Daesh.**

- **The Supplementary Estimates (C) include an increase of to CSIS' voted appropriations in order to address the crises in Iraq and Syria and the impacts on the region.**

- **Ongoing conflicts continue to shape the nature of the terrorism threat to Canada. Daesh, in particular, continues to inspire extremists with its violent ideology.**

- **The threat to Canada and Canadian interests posed by Daesh is international in scope. As such, a global reach is an absolute necessity in CSIS' efforts to investigate and respond to threats posed by Daesh to Canada and its partners.**

- **This funding will enhance CSIS' capacity to collect intelligence and advise Government on the security threats emanating from this complex environment.**

Supplementary Estimates (C), 2016-2017
Canadian Security Intelligence Service

BACKGROUND:

The 2016-2017 Supplementary Estimates (C) will result in a net increase of to CSIS' authorities.

- **Funding to address the crises in Iraq and Syria and the impacts on the region *(horizontal item)***

- **Funding to support enhanced national security review of foreign investment under *the Investment Canada Act***

- **Recovery of proceeds from the sale of homes purchased under the Homes Sales Plan**
  - Authority to recover proceeds deposited in the Consolidated Revenue Fund (CRF) for the sale of homes purchased by the Service from employees who are relocated to meet the Service's organizational needs.

- **Recovery of proceeds from parking fees collected**
  - Authority to recover proceeds deposited in the Consolidated Revenue Fund (CRF) from parking fees collected from Service employees and visitors to make parking operations fully "self-financing" as the market rate fees collected are sufficient to cover parking related costs.

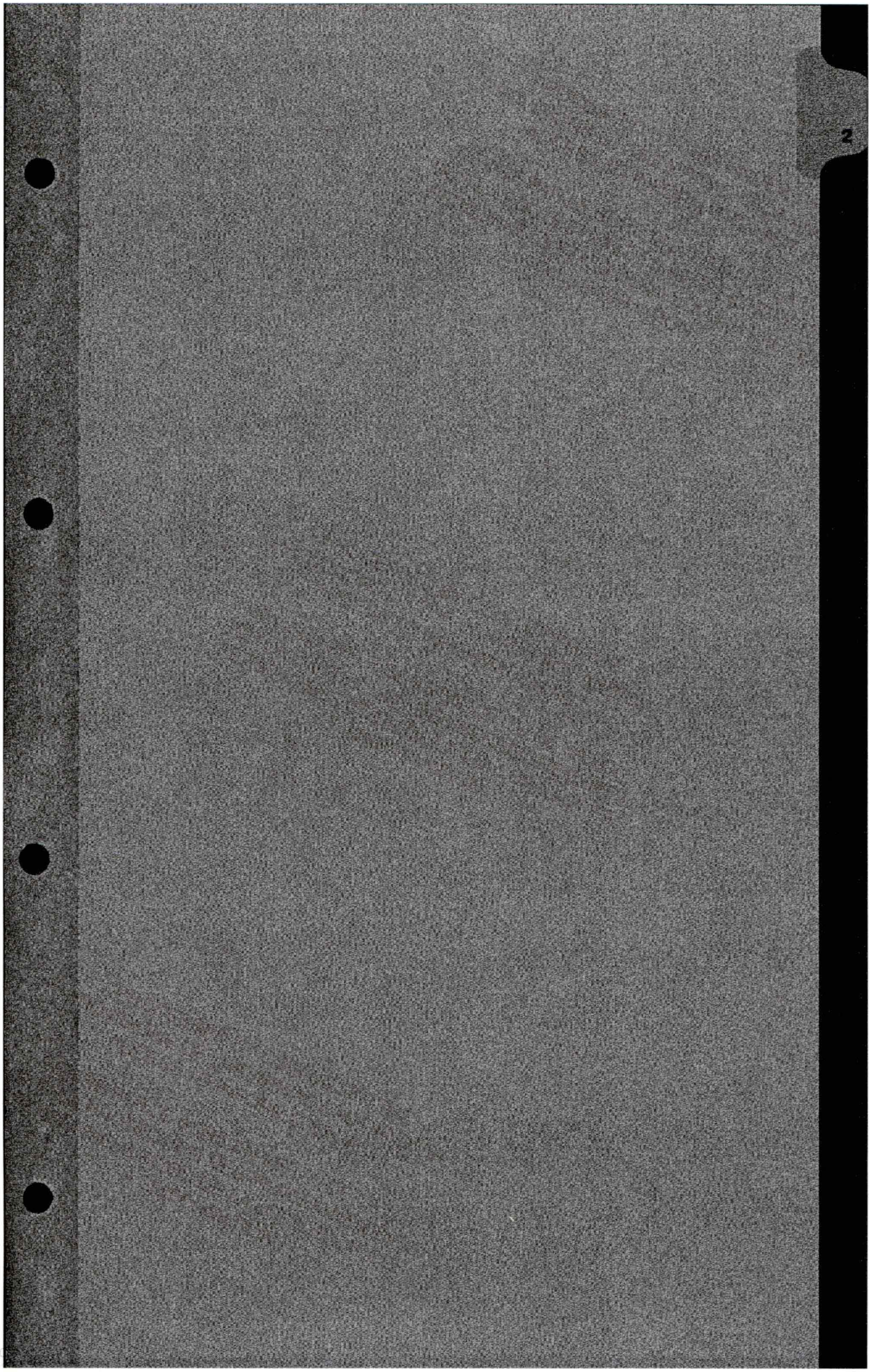
- **Recovery of costs related to security screening of employees at nuclear power plants and provincial government facilities**
  - Authority to recover the cost of security clearance at nuclear power plants and provincial government facilities. These entities are invoiced for the number of clearances processed and the funds received are deposited in the Consolidated Revenue Fund (CRF).

Gross Total Appropriations

- **Statutory Appropriations**
  - Contributions to Employee Benefit Plans (EBP).

- **Transfer from National Defence**
  - To support the Canadian Safety and Security Program, which provides science and technology solutions, support and advice for responding to the Government of Canada's public safety and security policy imperatives.

Total Increase to Supplementary Estimates (C)


2

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

A

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE: NATIONAL SECURITY CONSULTATIONS

IF ASKED ABOUT NEXT STEPS IN THE NATIONAL SECURITY CONSULTATIONS

- **Increased public awareness and dialogue is important for the national security and intelligence community. This consultation process, led by the Department of Public Safety, provided an opportunity for enhanced understanding of CSIS' role and mandate.**

- **The public conversation on national security is important to all Canadians and allows them to have input into the national framework designed to ensure their safety and security. Canada's national security laws and policies should reflect the rights, values and freedoms of Canadians.**

- **CSIS has been actively supportive of Public Safety's work in this regard, and will support the Minister during the Parliamentary process as appropriate.**

IF ASKED ABOUT RECENTLY RELEASED REPORTS BY HOUSE OF COMMONS COMMITTEES (SCISA AND NATIONAL SECURITY FRAMEWORK)

- **I understand that the Committee has released the report and that the next step is for the Government to consider its response.**

- **As such, it would be inappropriate for me to comment on the specific recommendations of the committee's report at this time.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE: THREAT REDUCTION

IF ASKED ABOUT THREAT REDUCTION MEASURES

- **The Service obtained its threat reduction authority with the passing of Bill C-51 in Summer 2015, which, amongst other things, amended the *CSIS Act*.**
- **While we always consider the range of possible response options, CSIS has used its new threat reduction mandate to reduce threats to the security of Canada. This has always been done in consultation with domestic partners.**
- **It must be noted that SIRC has expressed its satisfaction with the rigorous governance framework that the Service has implemented to operationalize this new threat reduction mandate.**

IF ASKED ABOUT THE USE OF WARRANTED MEASURES

- **The *CSIS Act* clearly identifies when CSIS must seek a warrant to reduce a threat and what conditions must be satisfied for the Court to authorize certain measures. CSIS would be required to obtain Ministerial approval before seeking a warrant.**
- **I must note that the Service's threat reduction mandate is still relatively new and CSIS has taken an incremental approach to relying on this new authority to ensure its operationalization conforms with all policy and legislative requirements. As such, the Service has not yet required a warrant to proceed with a threat reduction measure, however, this should not be taken to mean that a warrant will not be required in the future.**

ON IMPLEMENTATION OF TRA

- **The Service has developed a robust governance framework to give effect to the requirements set out in law and Ministerial Direction.**
- **Clear direction has been issued to all employees, complemented by formal training which is mandatory for all operational employees.**
- **A risk assessment is undertaken for each threat reduction measure. CSIS works with the Department of Justice to assess the application of Canadian law, including the *Charter*, and to determine if a warrant is required.**
- **Pursuant to Ministerial Direction, we also consult with partners, as appropriate, including Global Affairs Canada, the Royal Canadian Mounted Police, and the Communications Security Establishment.**
- **Since the amendments to the *CSIS Act* came into force in June 2015, the Service has approved a number of measures against a range of threats. None have required a warrant.**

ON THE NUMBER OF MEASURES TAKEN TO DATE

- **The Service has issued some two dozen approvals for threat diminishment measures since the mandate came into effect.**
- **Every day, the Service gains experience in identifying and developing these measures, and assessing their risks and impacts.**

ON SAFEGUARDS

- **Whereas we require "reasonable grounds to suspect" to initiate a national security investigation, the law requires that we have "reasonable grounds to believe" that a particular activity constitutes a threat to the security of Canada for threat reduction measures to be undertaken.**
- **The legislation also requires that threat reduction measures be reasonable and proportionate in the circumstances, having regard to the nature of the threat, the nature of the means to reduce the threat, and the reasonable availability of other means.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE : MOBILE DEVICE IDENTIFIERS (MDI)

IF ASKED WHETHER CSIS HAS USED MDI:

- **In the conduct of investigations, the Service uses a variety of methods to collect information. These are conducted in accordance with the CSIS Act, Ministerial Directives, robust internal policies, and when required, a warrant issued by the Federal Court.**

- **As indicated by our Minister, the Service uses technology, sometimes described in the media as "IMSI Grabbers", "Cell Site Simulators" or "Mobile Device Identifiers" under its lawful authorities in support of investigations.**

- **As our Director has previously stated, the number of terrorism-related threats, the speed at which they evolve, and the use of technology, has created some very real and complicated challenges for the Service.**

IF ASKED HOW OFTEN CSIS HAS USED MDIS:

- **For operational security reasons, CSIS is not prepared to elaborate further on how frequently this technology is used.**

IF ASKED WHETHER CSIS USES MDIS TO INTERCEPT THE CONTENT OF COMMUNICATIONS:

- **As the Minister has indicated, Canadian agencies use this technology in compliance with the law and lawful authorities.**

- **I can confirm that the equipment CSIS has is not capable of intercepting content.**

- **Without disclosing operational methods, I can say that CSIS, in determining the use of such investigative techniques, either relied on the authority provided by section 12 of the CSIS Act, or applied for a warrant to the Federal Court pursuant to section 21 of the Act, depending on the circumstances.**

- **However, in January 2017, the Service suspended the use of this technology while we undertake a review of the conditions and parameters regarding its use.**

IF ASKED WHY THE USE OF MDIS WAS SUSPENDED:

- **The policy and procedures for use of MDI devices to support CSIS operations are under internal review, as we assess our complex legal and operational environment. The use of the devices was suspended until the recommendations of the review are completed.**

IF ASKED WHEN MDIS ARE USED WITHOUT A WARRANT AND HOW OFTEN:

- **CSIS will apply for warrants where it is required to do so because of the manner and the degree in which an investigative technique may intrude upon the privacy of a person. In all cases, the Service would also rely on the authority to conduct investigations that is provided by the CSIS Act, including in particular section 12. For operational security reasons, the Service is not in a position to further discuss how or why we use this technology.**

IF ASKED WHETHER THE DATA COLLECTED USING MDIS HAS BEEN RETAINED BY THE OPERATIONAL DATA ANALYSIS CENTRE (ODAC):

- **Data collected using MDIs has not been provided to the Operational Data Analysis Centre for analysis.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE: FEDERAL COURT DECISION

IF ASKED ABOUT THE FEDERAL COURT DECISION – ANALYSIS OF NEWLY ACQUIRED ASSOCIATED DATA

- **As a result of the Federal Court decision, CSIS halted internal use and analysis of associated data obtained through warranted collection of communications to assess the impact of the decision and determine a way forward which complies with the federal court ruling.**

- **As of March 2017, CSIS implemented new retention practices for associated data collected under warrant. This will allow ODAC to recommence its analysis of *newly acquired* associated data in accordance with the Court's decision. However, such analysis has not yet recommenced.**

- **Where it is determined that the associated data is NOT of use to an investigation, it will be destroyed in accordance with the timeframes established by the Court.**

- **CSIS' historical associated data holdings remain fenced off, and unavailable for use, until a final decision is made regarding their disposition.**

- **It is important to underline that pursuant to s.12 of the *CSIS Act*, CSIS may collect, retain and analyze, to the extent that is strictly necessary, information and intelligence on threats to the security of Canada. This has not changed in recent years; CSIS has not gained new authorities to collect information.**

- **CSIS takes very seriously potential privacy considerations related to its work, and is committed to ensuring that its activities are transparent, accountable and in compliance with privacy legislation, guidelines and best practices.**

IF ASKED ABOUT THE ODAC PRIVACY IMPACT ASSESSMENT

- **A Privacy Impact Assessment on the Operational Data Analysis Centre was completed in August, 2010. CSIS is reviewing its PIA in light of current practices to determine if any updates or changes are required.**
- **CSIS advised the Privacy Commissioner of the Federal Court's decision immediately upon its release and stressed its commitment to work with his office to answer any questions related to the decision.**
- **The Office of the Privacy Commissioner has engaged CSIS on this matter and I can reassure the committee that CSIS officials are fully cooperating with the OPC.**

IF ASKED ABOUT THE FEDERAL COURT DECISION – BRIEFING THE COURT

- **CSIS agrees that the Court should have been informed earlier of its approach to data retention and the establishment of ODAC. It acknowledges that this was a significant omission.**
- **At no time did the Service deliberately withhold information from the Court. Indeed, the Decision notes that there was no evidence to suggest that this was case.**
- **Though CSIS agrees that the Court should have been informed earlier of its approach to data retention and the establishment of ODAC, key Government stakeholders were made aware of the existence of ODAC and its data analytics program.**
- **Indeed, former Ministers of Public Safety, the Office of the Privacy Commissioner, the Security Intelligence Review Committee and the Inspector General of CSIS were all briefed on CSIS' data analysis program.**
- **This does not, however, excuse CSIS' significant omission to inform the Court of this issue.**
- **We can and will do more to ensure that CSIS is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court warrants.**

IF ASKED ABOUT CSIS ACT AMENDMENTS

- **In its decision, the Federal Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.**
- **Ongoing assessment of the decision and its implications for CSIS investigations will help determine whether legislative action may be required. This is ultimately a decision for the Government.**
- **CSIS recognizes the importance of maintaining public trust and confidence in its activities, which is reinforced by transparent legislative authorities.**
- **As the Government contemplates its response to the national security consultations, this is an important opportunity to ensure that CSIS is meeting the dual objective of security and privacy, with the tools and authorities necessary to fulfill its mandate.**
- **Overall, CSIS must have clear authorities, combined with appropriate accountability and review mechanisms to ensure public confidence in our work.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE: SECURITY SCREENING AND ODAC

IF ASKED ABOUT WHETHER SECURITY SCREENING USES METADATA FROM ODAC:

- **CSIS uses a variety of investigative tools in support of its security screening program. This can include the use of data analytics to support security screening assessments.**

IF ASKED ABOUT WHETHER ODAC USES METADATA FROM SCREENING ASSESSMENTS:

- **Information from the Service's security screening program may be used in support of national security investigations, which is publicly acknowledged in the relevant CSIS Personal Information Bank.**

- **To be clear, ODAC does not use metadata from security screening assessments, as they do not contain metadata. Instead, security assessment information may be used in support of national security investigations, such as for corroborating a name or address.**

IF ASKED ABOUT ENGAGEMENT WITH THE PRIVACY COMMISSIONER ON THE USE OF SCREENING INFORMATION FOR NATIONAL SECURITY INVESTIGATIONS

- **I would note that SIRC reviewed the use of screening information by CSIS in its 2013-14 annual report, recommending that CSIS engage with the Office of the Privacy Commissioner on this matter.**

- **To this end, CSIS has held discussions with the Privacy Commissioner and has committed to address this issue in a related Privacy Impact Assessment, which is currently in development.**

- **CSIS takes very seriously all potential privacy considerations related to its work, and is committed to ensuring that its activities are transparent, accountable as well as in compliance with privacy legislation, guidelines and best practices.**

F

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE: FOREIGN INTERFERENCE

IF ASKED ABOUT FOREIGN INTERFERENCE IN CANADA'S POLITICAL SYSTEM, INCLUDING "SMEARING" THE FOREIGN AFFAIRS MINISTER

- **Any attempt by a foreign nation to target members of the Canadian Government through disinformation would undermine the integrity of Canadian political institutions.**
- **Allegations of interference in any of Canada's democratic institutions or processes by a foreign state would be taken very seriously by CSIS .**
- **While I cannot speak to such an occurrence for operational reasons, these actions would constitute a threat to the security of Canada as defined by the *CSIS Act*.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

HOT ISSUE: SURVEILLANCE OF SENSITIVE SECTORS

IF ASKED ABOUT THE SURVEILLANCE OF JOURNALISTS / MEDIA OUTLETS

- **Freedom of the press is a fundamental Canadian value and CSIS recognizes and respects the role that journalists play, both in informing Canadians, and in contributing to the conversation on national security.**
- **As we have indicated previously, CSIS does not investigate journalists to determine their sources.**
- **While I cannot go into specifics regarding the subjects of our investigations, the *CSIS Act* is very clear: CSIS can only investigate activities which we have reason to suspect constitute a threat to national security.**
- **CSIS has a duty to identify and advise Government of threats to our national security, and we exercise our authorities set out in law to fulfill this mandate.**
- **Any individual engaged in threat-related activities may be subject to this kind of lawful investigation, irrespective of their profession.**
- **As such, in fulfilling its mandate, there may be instances in which the Service's lawfully authorized investigations come into contact with individuals associated with Canadian fundamental institutions, such as the media.**
- **Any investigation by the Canadian Security Intelligence Service that affects a fundamental societal institution is subject to additional safeguards and requirements outlined in Ministerial Direction.**
- **In a 2009-10 review, the Security Intelligence Review Committee recognized that CSIS exercises special care in the conduct of operations that affect – or even appear to affect – fundamental institutions.**

IF ASKED ABOUT THE SURVEILLANCE OF PROTEST MOVEMENTS AND THE ENERGY SECTOR

- **Members, I would like to emphasize that CSIS' activities, including the collection of information, continue to be governed by the *CSIS Act*, which explicitly prohibits the investigation of lawful protest and dissent.**

- **CSIS is authorized to collect information, to the extent that it is strictly necessary, on activities suspected of constituting a threat to the security of Canada.**

- **CSIS collects and analyzes threat-related information, which is typically disseminated to government partners through intelligence reports and other intelligence related briefings.**

- **While I cannot publically disclose our investigational interests, I can say that CSIS' threat assessment for the energy sector remains constant. Globally, the energy sector remains a significant target for cyber-espionage, and cyber intrusions, orchestrated by hostile actors.**

- **Clearly this kind of activity is of concern. Canada is not immune to such attacks and countering these threats is a key national security priority.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
REVISE PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCES
A L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
REVISE PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCES
A L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

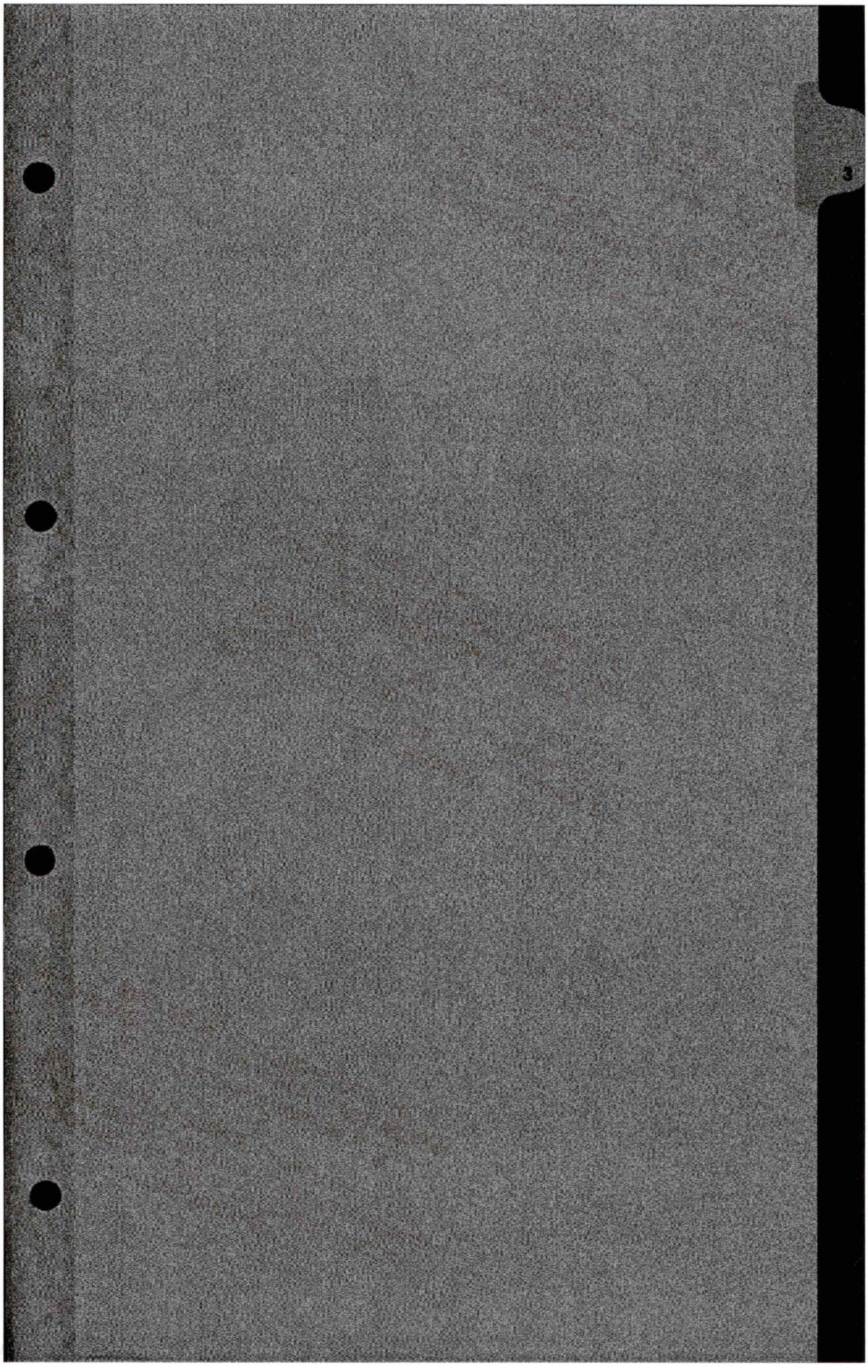
Committee Note

HOT ISSUE: MEDIA REPORTS ON MONTREAL TRUDEAU AIRPORT

ISSUE: What are the Service's roles and responsibilities towards the Transportation Security Clearance Program? What can the Service say about recent reporting on radicalized individuals working at the Montreal airport?

IF ASKED ABOUT CSIS' SCREENING ROLE:

- **I am aware of the recent media reporting on individuals working in secure areas of the Montreal Trudeau Airport.**
- **I would direct any specific questions about the Transportation Security Clearance Program, including the status of individuals' clearances, to my Transport Canada colleagues.**
- **I must also note that any information regarding CSIS investigations is classified. As such, I am unable to comment on any specific individuals or cases in a public forum.**
- **However, I want to reassure Members that we work closely with Transport Canada throughout the assessment process to ensure they have information about potentially serious national security concerns, given the vital public safety considerations at airports.**
- **CSIS supports Transport Canada's decision-making on the granting, denial or revocation of security clearances by providing security assessments in accordance with the relevant provisions of the *CSIS Act*.**
- **Further, there are mechanisms in place to ensure that if either CSIS or Transport Canada become aware of threat-related information relevant to an individual's clearance, investigations can be re-opened.**
- **Should CSIS re-open a clearance for investigation, we would inform our government partner of this action accordingly.**
- **I would also like to stress that CSIS may only investigate cases when it has the legal authority to do so. Meaning, out of respect for the rights of Canadians – including their freedom of expression - there must be a reason for the Service to undertake such an investigation.**


3

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

A

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

FEDERAL COURT DECISION

ISSUE: How is CSIS responding to the decision? Why did CSIS not inform the Court of its new position on the retention of associated data and the creation of the Operational Data Analysis Centre? Were the Government or review bodies informed? How does CSIS conduct data analytics and why? What are the privacy implications for Canadians? Is the CSIS Act dated? Will the Government consult Canadians on CSIS' data analytic activities?

- **In October 2016, the Court determined that CSIS' retention of associated data linked to third party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs, was not compliant with the *CSIS Act*.**
- **The Service accepted the Court's ruling and took immediate actions to halt all analysis of associated data while it assessed the Court's findings. A team was created to assess the implications of the decision and implement required technological changes.**
- **As has been stated previously: CSIS collected this associated data legally, through warrants issued by the Federal Court. The Court's key concern related to CSIS' *retention* of non-threat-related associated data linked with third party communications.**
- **With respect to duty of candour, I am working with the Deputy Minister of Justice to ensure that we meet our obligations to the Court in matters of transparency and duty of candour.**
- **I wish to reiterate that CSIS takes very seriously concerns raised in the Federal Court's decision and it is committed to ensuring that its activities comply with this new interpretation of the *CSIS Act*.**

ON CSIS' RESPONSE

- **CSIS agrees that the Court should have been informed earlier of its approach to data retention and the establishment of ODAC. It acknowledges that this was a significant omission.**
- **At no time did the Service deliberately withhold information from the Court. Indeed, the Decision notes that there was no evidence to suggest that this was case.**

- **CSIS' data exploitation program was known publically. In its 2008 Public Report, CSIS very briefly referenced ODAC, noting that it provides support to the Service's operational branches by performing advanced analysis of data that is collected on subjects of investigation.**
- **In addition, Ministers of Public Safety, the Office of the Privacy Commissioner, the Security Intelligence Review Committee and the Inspector General of CSIS were all briefed on the existence of ODAC and the added value of data analytics to CSIS investigations.**
- **I wish to stress that I am committed to ensuring that CSIS meets its obligations to the Court in matters of transparency and duty of candour.**

ON ANALYSIS OF NEWLY ACQUIRED ASSOCIATED DATA

- **As a result of the Federal Court decision, CSIS halted internal use and analysis of associated data obtained through warranted collection of communications to assess the impact of the decision and determine a way forward which complies with the federal court ruling.**
- **As of March 2017, CSIS implemented new retention practices for associated data collected under warrant. This will allow ODAC to recommence its analysis of *newly acquired* associated data in accordance with the Court's decision.**
- **Where it is determined that the associated data is NOT of use to an investigation, it will be destroyed in accordance with the timeframes established by the Court.**
- **CSIS' historical associated data holdings remain fenced off, and unavailable for use, until a final decision is made regarding their disposition.**
- **It is important to underline that pursuant to s.12 of the *CSIS Act*, CSIS may collect, retain and analyze, to the extent that is strictly necessary, information and intelligence on threats to the security of Canada. This has not changed in recent years; CSIS has not gained new authorities to collect information.**

- **CSIS takes very seriously potential privacy considerations related to its work, and is committed to ensuring that its activities are transparent, accountable and in compliance with privacy legislation, guidelines and best practices.**

ON THE PRIVACY OF CANADIANS / ENGAGEMENT WITH THE OFFICE OF THE PRIVACY COMMISSIONER

- **The Federal Court did not speak to the privacy considerations of the retention of non-target, non-threat-related associated data.**
- **It is important to note that associated data does not reveal the purpose of a communication, nor any part of the content. On its own, it does not identify individuals who are party to a communication.**
- **That said, CSIS takes very seriously potential privacy considerations related to its work, and is committed to ensuring that it undertakes its activities in compliance with privacy legislation, guidelines and best practices.**
- **It must be noted that a Privacy Impact Assessment on the Operational Data Analysis Centre was completed in August, 2010. CSIS is reviewing its PIA in light of current practices to determine if any updates or changes are required.**
- **I advised the Privacy Commissioner of the release of the Federal Court's decision immediately upon its release and stressed my commitment to work with his office to answer any questions related to issues raised in the decision.**
- **The Office of the Privacy Commissioner has engaged CSIS on this matter and I can reassure the committee that my officials are fully cooperating with the OPC on this matter.**

ON BRIEFINGS TO THE MINISTER

- **At various points since its creation, different Ministers of Public Safety were informed of the existence of ODAC and the added value of data analytics to CSIS investigations.**

- **In 2006, the necessity of creating ODAC and a data analytic capability was described to the Minister of Public Safety. It was, at the time, noted that a basic requirement of ODAC would be the ability to retain data for extended periods of time.**
- **From 2007 to 2010, CSIS provided information on ODAC's work in its then s.33(1) reports to the Minister of Public Safety. Additionally, in 2010, CSIS provided the Minister of Public Safety with a verbal briefing on ODAC. The program was again referenced in 2014 and 2015, as part of CSIS' s.6(4) report to the Minister.**

ON THE INTERACTION WITH REVIEW BODIES

- **Over time, CSIS has interacted with different review bodies in relation to the existence of ODAC and the value added of data analytics to CSIS investigations.**
- **In 2007, CSIS responded to a SIRC request for information on ODAC and discussed the analysis of metadata as an investigative tool.**
- **In 2010, CSIS submitted a Privacy Impact Assessment on the ODAC program to the Office of the Privacy Commissioner. As I have noted, I have advised the OPC of the decision and have directed my officials to fully cooperate with the OPC to address any questions they may have.**
- **In 2011, CSIS provided a verbal briefing on ODAC to the Inspector General of CSIS.**
- **In 2014, CSIS provided SIRC with a detailed verbal briefing on ODAC's use of metadata.**
- **Though review bodies were, on numerous occasions, advised of the existence of ODAC, as well as the added value of data analytics to CSIS investigations, such interactions did not occur with the Federal Court.**
- **In March 2015, SIRC reviewed CSIS' use of associated data as well as other data (which SIRC referred to globally as metadata). Its findings were reported in its 2014-15 annual report, which was tabled in Parliament in January 2016.**

- **SIRC did not conclude that CSIS' use of metadata was illegal. It did, however, conclude that the Service's transparency with the Federal Court, as it pertained to the use of metadata, was insufficient.**

ON THE INTERACTION WITH THE FEDERAL COURT

- **The *CSIS Act* defines the Service's relationship with the Court. The means to approach the Court is through warrant applications, which creates a very focused type of interaction.**
- **In 2011, CSIS advised the Federal Court that it amended the wording of warrant conditions, but the Court found that this submission did not adequately address the distinction between the content of communications from the associated data of communications.**
- **CSIS accepted the Court's finding in this regard. The development of this capability has evolved over time, as has our understanding of our obligations towards the Court.**

ON DATA ANALYTICS AND ODAC – RATIONALE

- **To derive more value from the data already being collected under warrant using data exploitation techniques, CSIS established ODAC in 2006.**
- **Data analytics employs computers to analyze data and discover linkages, trends and patterns. These techniques enable humans to make sense of volumes of information that could not be processed without a computer's assistance.**
- **Data analytics enables the Service to effectively analyze threats to the security of Canada over time. It can provide insight into contacts between subjects of investigation; identify new leads and intelligence gaps; provide context and understanding to operations and protect the security of operations and the safety of employees engaged in operations.**
- **The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard.**

- **Associated data refers to information associated to a communication intercepted pursuant to a warrant. Associated data is the context, not the content of a communication. Such data is used by computer systems to identify, describe, manage or route communications across a network.**
- **For example, associated data is data derived from a communications event. It can refer to, amongst other things, an internet protocol address, a phone number, the time of a transmission or the location of a device.**
- **The exploitation of associated data enhances the Service's ability to effectively investigate threats to the security of Canada. It assists in identifying patterns of movement, contacts and links that are otherwise unidentifiable.**

ON CSIS ACT AMENDMENTS

- **In its decision, the Federal Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.**
- **Ongoing assessment of the decision and its implications for CSIS investigations will help determine whether legislative action may be required. This is ultimately a decision for the Government.**
- **CSIS recognizes the importance of maintaining public trust and confidence in its activities, which is reinforced by transparent legislative authorities.**
- **As the Government contemplates its response to the national security consultations, this is an important opportunity to ensure that CSIS is meeting the dual objective of security and privacy, with the tools and authorities necessary to fulfill its mandate.**
- **Overall, CSIS must have clear authorities, combined with appropriate accountability and review mechanisms to ensure public confidence in our work.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

B

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

TERRORISM

ISSUE: What is the domestic environment for terrorism in Canada? What is being done about radicalization in Canada? How does the international context relate to what is happening in Canada? How many Canadians abroad are engaged in terrorist activity? How many returnees? How is CSIS countering the terrorism and extremist threat?

- **The primary terrorist threat to Canadians remains extremists who are motivated to carry out deadly attacks in our communities.**
- **Radicalized individuals in Canada have planned attacks, sent money and supplies to violent extremist groups, and sought to recruit members of their communities, particularly youths.**
- **Conflicts abroad, particularly those in Iraq and Syria, continue to inspire attempts to make attacks on Canadians.**
- **Canadians were used by extremist groups in suicide missions, as recently as March 2017, when a Daesh recruit, Abu-Maliha al-Kanadi, conducted a suicide bombing against Iraqi Forces in Mosul, Iraq.**
- **CSIS considers a range of options when dealing with extremists who are in, leaving or returning to Canada, in consultation with partners and allies.**
- **We also consistently rely upon the vigilance and cooperation of Canadians in working to prevent attacks inside our country.**

ON THE DOMESTIC ENVIRONMENT

- **The terrorist threat level in Canada remains at MEDIUM, meaning that there is sufficient credible information that a violent act of terrorism could occur.**
- **At the current threat level, a terrorist incident could be simple and spontaneous, or have taken months or years to plan, employing extensive logistics and sophisticated tradecraft.**

ON RADICALIZATION

- **The narrative that the West is at war with Islam continues to exert a powerful influence in radicalization both in our communities and online.**
- **Given the mandate of the Service, our focus is on individuals who are seeking to act on, or assist others, in carrying out violent attacks.**
- **The Service has unique insight into the small number of Canadians who embrace terrorism, and CSIS continues to work with partners to better understand radicalization as it develops into violence in the Canadian context.**
- **The Service works to identify and determine when an individual is moving from holding extremist ideas to taking action, which assist efforts to detect and prevent acts of terrorism.**

ON THE INTERNATIONAL CONTEXT

- **Violence conducted and inspired by Daesh and Al Qaeda has had a devastating impact on the international stage.**
- **Cooperation with our partners is of utmost importance as we play our role in protecting Canadians.**

ON TERRORIST TRAVEL

- **There remain approximately 180 individuals with a Canadian link who have left Canada in support of terrorist activities.**
- **Travellers participate in a range of activities depending on their abilities and contacts; paramilitary training, suicide missions, logistical and financial support, even translation and propaganda.**

ON NUMBERS ABROAD

- **Of the approximately 180 individuals abroad, over half are known to be in Syria or Iraq, though precision is challenging due to a porous border and shifting checkpoints.**

- **These numbers do not include returnees, or individuals in Canada who are engaged in activities in support of terrorism.**

- **Given the significant operational challenges associated with counter terrorism investigations of Canadians abroad, CSIS continues to be concerned about the number of individuals that we are not aware of, and those for whom we have incomplete information.**

ON RETURNEES

- **The Service is currently aware of approximately 60 people who have returned to Canada after having travelled overseas in support of terrorism.**

- **Extremists returning to Canada could pose a threat to public safety, and there are important concerns regarding their reintegration into society.**

- **Returnees have responded to their life in Canada in a variety of ways. While some return to regular life, others have become key contacts for radicalization, terrorist travel or financing, both online and in their communities.**

- **Knowing the mentality and choices of returnees can vary significantly, CSIS tries to maintain situational awareness to rule in or out potential threats.**

- **It is worth noting that the number of people returning from the Syrian conflict zone has decreased, which can be attributed to Daesh's tight control and intense scrutiny over their recruits for potential desertion.**

ON RESPONSE OPTIONS

- **There are a range of options to consider, often in consultation with partners. A coordinated, national response to returnees requires the cooperation of all implicated departments and agencies.**
- **CSIS will often make the decision to investigate further, to determine if there is indeed the possibility of criminal activity.**
- **The Service at times may make the decision to share critical information with our partners to inform a criminal investigation or enforcement action (eg, citizenship, immigration decisions, as well as the prevention of travel in support of violent extremism).**

- **To protect the information that we hold, and so as not to disrupt ongoing investigative work, I am not at liberty to discuss the details of specific cases.**

ON THE PUBLIC THREAT REPORT

- **CSIS contributes to The Public Report on the Terrorist Threat to Canada at several stages in the process, and welcomes the opportunity for transparency on non-operational topics that are also intrinsic to the national security landscape in Canada.**
- **CSIS appreciates the role of public reports in informing Canadians on threats to the security of Canada, and building an understanding of global terrorism.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

FOREIGN INTERFERENCE

ISSUE: Why are investigations on foreign intelligence activities a priority for the Service? Is CSIS involved in the review of foreign investments?

- **Certain foreign states continue to be involved in espionage to gather political, economic and military information in Canada through clandestine means. Such states pursue their own national interests through covert means, targeting Canadian businesses, political institutions and members of various diaspora communities in Canada, and, ideally from their perspective, recruiting "insiders".**
- **Cyber operations provide another means of espionage, as the theft of information and compromise of systems belonging to Canadian private and public sector entities can be done clandestinely, including from outside Canada.**
- **Countries targeting their diaspora here in Canada is a key aspect of foreign interference. It can involve intimidating, coercing and threatening members of many communities to secure their support for foreign agendas.**
- **One of Canada's strengths--advanced industrial and technological capabilities, combined with expertise in a number of sectors—unfortunately also continues to make our country an attractive target for foreign actors and intelligence services seeking to gather information, or influence and interfere in Canadian political and economic affairs in particular.**

FOREIGN INFLUENCED ACTIVITY

- **Foreign influenced activity, which includes foreign interference, is the clandestine influence and direction of political or other Government actors to the detriment of Canadian interests and may involve a threat to persons in Canada, including members of a foreign state's diaspora community.**

- **When diaspora groups in Canada are subjected to clandestine and deceptive manipulation or intimidation by foreign states seeking to gather support for their policies, or to mute criticism, these activities constitute a threat to Canadians and the sovereignty of Canada.**

- **Such investigations are highly sensitive but highly important, which is why when CSIS was created 30 years ago, we were authorized to investigate this threat.**

FOREIGN INTERFERENCE IN CANADA'S POLITICAL SYSTEM

- **Any attempt by a foreign nation to target members of the Canadian Government through disinformation would undermine the integrity of Canadian political institutions.**

- **Allegations of interference in any of Canada's democratic institutions or processes by a foreign state would be taken very seriously by CSIS .**

- **While I cannot speak to such an occurrence for operational reasons, these actions would constitute a threat to the security of Canada as defined by the *CSIS Act*.**

FOREIGN INVESTMENT

- **While foreign investment is a key driver of Canada's economic prosperity, foreign investment does have the potential to gravely impact national security interests through the acquisition of sensitive intellectual property for foreign use or foreign state control over strategic resources.**

- **To assess such impacts, the *Investment Canada Act* authorizes the Government to review foreign investments on national security grounds.**

- **CSIS works with partners to provide advice in support of this process whereby the Governor in Council may stop or impose mitigation conditions on investments that could or would be injurious to Canada's national security.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

CYBER SECURITY

ISSUE: Can you explain what CSIS is doing to protect Canadians against cyber threats?

- **Canada remains a target for malicious, offensive cyber activities by hostile actors, who target the networked infrastructures of both the public and the private sectors, as well as the personnel using these systems.**
- **Hostile cyber actors can include states, criminals, politically or ideologically motivated groups or individuals, and extremist groups.**
- **Cyber operations are efficient, cost-effective, and most importantly, deniable.**
- **In an increasingly digitalized world, and with the central role technology plays in the lives of Canadians, the range and scale of cyber threats to Canada, Canadians, and Canadian interests will only increase.**
- **Hostile state-sponsored actors use cyber tools and capabilities to advance their economic, military, and political agendas.**
- **Once compromised, Canadian digital infrastructure may be used to launch attacks against public and private sector entities abroad, damaging Canada's international reputation.**

ON NATIONAL SECURITY FRAMEWORK - CYBER

- **CSIS is mandated to investigate activities which are suspected of constituting a threat to the security of Canada, including those emanating from cyberspace.**
- **CSIS investigates and assesses national security cyber threats and provides advice to Government partners, contributing to efforts to protect Canada from cyber threats.**
- **CSIS works closely with other Government partners – such as the RCMP, the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre to respond to cyber threats to Canada.**

- **CSIS was a key contributor to Canada's 2010-2015 Cyber Security Strategy.**

ON CSIS' USE OF TRA AND OFFENSIVE CYBER OPERATION

- **The internet represents a unique theatre of operations with its own dynamics and challenges.**
- **The internet itself is value-neutral and remains a tool and method of communication, used for both legitimate and nefarious purposes. CSIS is only interested in activity of the latter sort that represents a threat to national security as defined in the *CSIS Act*.**
- **While I cannot speak to tradecraft, I can state that any potential disruptive cyber activities undertaken by the Service would operate under the same stringent authorization requirements as other threat reduction measures, and would be conducted in consultation with CSE, as appropriate.**

ON CYBER REVIEW

- **As you know, the Government of Canada has reviewed its measures to protect critical infrastructure and Canadians from cyber threats. Along with Public Safety's partner departments and agencies, CSIS is engaged in this review, and supports efforts to evaluate and refresh Canada's cyber security strategy.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
REVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
REVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

CSIS COOPERATION WITH FOREIGN AGENCIES

ISSUE: How is CSIS working with partners to keep Canada safe? How are such foreign arrangements established and assessed? How does CSIS assess human rights issues with respect to its relationships with foreign agencies?

- **CSIS maintains a well-established network of relationships with foreign agencies abroad.**
- **CSIS has more than 300 foreign relationships in some 150 countries, each authorized by the Minister of Public Safety and supported by the Minister of Foreign Affairs, in accordance with s.17 of the CSIS Act.**
- **In response to the evolving threat environment, and particularly following the events of 9/11, CSIS needed to expand its international presence and access to foreign agency intelligence to address increased threats to Canadians and Canada's national interests.**
- **CSIS also has officers stationed abroad whose role is to collect and, when required, share security intelligence information related to threats to Canada, its interests and its allies with host agencies.**
- **CSIS remains committed to collecting security intelligence information — within Canada and abroad — on threats to Canada, its interests and those of our allied international partners.**

ON PROCESS FOR ESTABLISHING ARRANGEMENTS

- **As per s.17(1)(b) of the CSIS Act, the Service must obtain approval from the Minister of Public Safety to implement an arrangement with a foreign organization before it can begin exchanging classified information.**
- **As per s.17(1)(b) of the CSIS Act, the Minister of Public Safety must also consult with the Minister of Foreign Affairs before rendering a decision on such requests.**

- **The process to establish such an arrangement is stringent and takes into consideration a wide range of issues prior to the Service seeking Ministerial approval, including, for example: Canadian security requirements; the internal political situation and respect for human rights and the reliability of the agency.**

- **Additionally, prior to seeking the Public Safety Minister's approval for new arrangements, CSIS proactively consults with Global Affairs Canada.**

- **As per s.6(4) of the CSIS Act, I also provide an annual update to the Minister of Public Safety on the status of the Service's foreign arrangements inventory including the number of existing arrangements, as well as those implemented or altered during the fiscal year.**

ON FOREIGN COOPERATION

- **The increased 'globalization' of terrorism cannot be countered in isolation. Cooperation with foreign agencies provides CSIS access to timely information linked potential or specific threats, and allows the Service (and, in turn, the Government of Canada) to obtain information which might otherwise not be available.**

- **The threat posed by 'Foreign Fighters' is international in scope. As such, a global reach is an absolute necessity in our efforts to track — and attempt to thwart — threats posed by such individuals to Canada and its allies.**

- **CSIS actively cooperates with its foreign partners on this issue, including in relation to specific investigations, lessons learned, and assessments of the phenomenon.**

- **Through such relationships, CSIS advances its own investigations into threats to the security of Canada and its interests, and gains a greater understanding of the scope and nature of the foreign fighter phenomenon itself.**

ON HUMAN RIGHTS AND INFORMATION SHARING

- **CSIS opposes in the strongest possible terms the mistreatment of any individual by a foreign agency, and in all situations, we must and do comply with Canada's laws and legal obligations in sharing information with foreign entities.**

- **The human rights reputations of the agencies with which CSIS engages is not something which the Service takes lightly. CSIS must assess and mitigate potential risks of sharing information with foreign entities, always cognizant of the fact that our first responsibility is to the Canadian people and their safety.**

- **CSIS continuously assesses all of its foreign arrangements, including human rights reputations of the country, and more specifically, of the agency with which it has established such arrangements.**

- **As part of this assessment process, CSIS regularly reviews various government and non-government human rights reports and assessments for all countries with which the Service has implemented Ministerially-approved arrangements. We also liaise with allied foreign counterparts in support of such assessments.**

- **In addition to specific protocols for information sharing, the way in which we establish and manage foreign arrangements is designed to mitigate risk.**

- **It is noteworthy that, in 2015, the Security Intelligence Review Committee (SIRC) found that the Service implemented a sound information sharing framework which includes a robust decision making process.**

ON MINISTERIAL DIRECTION

- **Ministerial Direction clearly states that in sharing information, CSIS must act in a manner that complies with Canada's laws and legal obligations and avoid any complicity in mistreatment by foreign entities.**

- **To do so, CSIS must assess and mitigate potential risks of sharing with foreign entities, as well as the accuracy and reliability of information received.**

- **We have very specific direction in place to do so, supported by a detailed decision-making process, supported by a senior-level committee that is convened as required. In this year's report, SIRC found the range of participants around the table fostered substantive discussion and provided for a rigorous decision-making process.**

- **There are also clear requirements to refer such decisions for more senior approval, as required, including to the Director and the Minister.**

- **Exchanges with foreign agencies may also be incremental in nature, in order to gauge the reliability of the agency and the usefulness of such an arrangement. Exchanges are also commensurate with the degree of trust established over a period of time and reflective of the political and human rights climate within the country in question.**

- **That said, if CSIS received information indicating Canadian lives may be at risk, we would be negligent not to assess and attempt to corroborate it in order to prevent a direct and timely security threat, such as terrorist attack, against Canada or its interests regardless of the information's origins.**

ON IDENTIFYING SPECIFIC ARRANGEMENTS

- **CSIS' relationships with its foreign partners are classified and not publicly identified.**

- **The majority of intelligence services worldwide do not wish to publicly divulge the list of foreign agency partners with which they liaise on security intelligence matters. Publicly divulging the existence of such arrangements could seriously hamper the Service's ability to liaise with such agencies in order to obtain security intelligence information relevant to the national security of Canada and Canadian interests.**

- **That said, our relationships with our close, traditional Five-Eyes partners – the United States, United Kingdom, Australia, and New Zealand – are widely known. The Five-Eyes is an invaluable network for the Canadian intelligence community. Without the benefits of this cooperation, Canada would suffer from significant intelligence gaps.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

SECURITY OF CANADA INFORMATION SHARING ACT

ISSUE: Does the SCISA alter CSIS' mandate? What safeguards are in place to protect the privacy rights of Canadians? What has CSIS done to implement the SCISA? What has been CSIS' experience to date? Has SCISA expanded the scope of information it can collect from Global Affairs Canada?

- **Timely access to reliable information is critical to the success of the Service's lawful investigations and enhances the advice we provide to Government.**
- **CSIS investigates threats to the security of Canada as defined in the *CSIS Act.***
- **The *Security of Canada Information Act* (SCISA) does not expand the range of threats CSIS is authorized to investigate, nor does it in any way alter CSIS' mandate.**
- **Rather, it creates an explicit authority for departments to share with CSIS. This means that departments have a clear, explicit authority to share information with CSIS under SCISA where it is relevant to our mandate.**

ON THE HOUSE OF COMMONS COMMITTEE ON ACCESS TO INFO, PRIVACY AND ETHICS REPORT

- **I understand that the Committee has released the report and that the next step is for the Government to consider its response.**
- **As such, it would be inappropriate for me to comment on the specific recommendations of the committee's report at this time.**

ON DEFINITIONS AND THRESHOLDS (SCISA, CSIS ACT):

- **SCISA provides an explicit authority for Government departments to share information with designated recipients where relevant to activities that undermine the security of Canada.**
- **The definition of "activities that undermine the security of Canada" does not affect the definition of threats to the security of Canada for the purpose of CSIS investigations nor does it alter or expand the Service's authority to collect information.**

- **CSIS' activities, including the collection of information, continue to be governed by the *CSIS Act*, which explicitly prohibits the investigation of lawful protest and dissent – SCISA does not change that.**

- **CSIS is designated as a recipient institution, given that its duties and functions – to investigate threats to the security of Canada – are aligned with the definition of "activities that undermine the security of Canada" in SCISA.**

- **While CSIS' duties and functions fall within this definition, any collection of information by CSIS must comply with obligations under the CSIS Act – that is, CSIS is authorized to collect information only to the extent that is strictly necessary to investigate threats to the security of Canada.**

ON THRESHOLDS (SCISA, CSIS ACT):

- **The legislation clearly articulates the requirements to meet before any department can disclose information.**

- **As we negotiate new arrangements with partners and provide guidance to employees, we carefully reflect on the thresholds both for disclosure and collection; these are meaningful thresholds that are carefully implemented.**

- **We can reasonably meet the relevant threshold, which is useful from an investigative perspective. To achieve a "necessity" threshold, could be challenging. It is not always possible to state with certainty that a piece of information is "necessary" to an investigation ahead of time, nor what would have happened without it.**

- **I understand, however, this matter is subject to ongoing public consultation.**

ON DISCRETIONARY VS. MANDATORY DISCLOSURE

- **Disclosure under SCISA is discretionary, which means it does not create an obligation or mandatory requirement for institutions to share information with CSIS.**

- **Though CSIS may receive information pursuant to SCISA, CSIS discloses information in accordance with the CSIS Act.**

- **While we regularly cooperate with partners, including, for example, the RCMP, each disclosure is carefully considered in light of operational and privacy requirements. In all cases, public safety is paramount.**

ON PRIVACY CONSIDERATIONS

- **SCISA does not create new or broader collection authorities for the Service. CSIS is still bound by its collection authorities in the *CSIS Act* and information collected must be strictly necessary to the investigation of threats to the security of Canada.**

- **CSIS is also subject to the requirements of the *Privacy Act,* which applies to the collection and disclosure of personal information, including that which is shared pursuant to SCISA.**

- **CSIS is implementing SCISA on a partner by partner basis to fully consider potential privacy implications associated with each relationship.**

ON SAFEGUARDS AND ACCOUNTABILITY

- **SCISA does not compel departments and agencies to share information.**

- **How and what information is shared under this new Act is carefully assessed by the originator and the recipient. Originators maintain discretion on whether to share, as well as how and what information is shared.**

- **We have worked with partners on a priority basis to consider our information sharing relationships and how to effectively integrate this new authority.**

- **To date, we have signed one information sharing arrangement with Global Affairs Canada to ensure appropriate protocols are in place. We also developed a new protocol with the Canada Revenue Agency in light of changes to the *Income Tax Act*, with an arrangement currently under development.**

- **It should also be noted that CSIS activities can be – and are – reviewed by the Privacy Commissioner.**

ON ONWARD DISCLOSURE

- **CSIS carefully manages its information sharing with partners.**
- **The issue of onward disclosure is one that we directly addressed in our Information Sharing Arrangement with Global Affairs Canada. In this case, written consent would be required prior to disseminating information to a third party.**
- **This is one of the key considerations in the development of such arrangements.**

ON CHANGES TO THE INCOME TAX ACT

- **CSIS used to collect taxpayer information under warrant, by statute.**
- **With amendments to the *Income Tax Act*, a warrant is no longer required. CSIS and the Canada Revenue Agency have worked together to develop a new protocol.**
- **Any questions on the rationale for these legislative changes should be directed to Public Safety or to the Canada Revenue Agency, as CSIS was not involved in those deliberations.**

ON THE PRIVACY COMMISSIONNER'S REPORT

- **As part of its Annual Report, the Office of the Privacy Commissioner reviewed the implementation and application of SCISA during the first six months after its coming into force. CSIS is mentioned as one of five institutions having received information under SCISA during this time.**
- **The entities surveyed in the report indicated that information had been shared in accordance with SCISA.**
- **CSIS fully cooperated, and continues to do so, with the Office of the Privacy Commissioner in the context of its review of personal information handling practices.**

- **SCISA is being examined as part of the ongoing national security consultations. CSIS remains prepared to support this process, as appropriate, and will, of course, comply with any resulting amendments.**

ON IMPLEMENTATION

- **CSIS has adopted a strategic approach to implementing SCISA by engaging partners on a priority basis. These partners were identified based on operational needs and requirements.**

- **This practical approach considers the particularities of each relationship, including policy, operational and privacy considerations. It has also allowed CSIS to review current relationships, identify opportunities for improvement and ensure relationships are adapted as necessary.**

- **CSIS has signed one SCISA-specific arrangement with Global Affairs Canada and adopted related protocols.**

ON EXPERIENCE TO DATE

- **While I cannot speak to specific details, I can confirm that CSIS has received information under SCISA. However, there has been no "wholesale" transfer of information under SCISA.**

- **We moved quickly to review existing relationships with priority partners.**

- **In the case of Global Affairs Canada, for example, SCISA offered an opportunity to overcome challenges identified by both organizations and by SIRC, allowing us to put in place clear protocols anchored in a new legislative authority.**

- **Though there has not been a "flood" of new sharing, I would suggest this is because we have adopted a measured approach to ensure that all relevant legal, policy, privacy and operational considerations are assessed.**

ON REQUIREMENT FOR SCISA (BN)

- **A CSIS briefing note, written prior to Bill C-51 and in support of a senior management meeting on national security information sharing, was released through ATIP.**

- **As a result of the application of redactions, the advice provided in the note has been misinterpreted. The note identified existing gaps and the benefits of SCISA. However, given the uncertainty of the legislative process, the note also suggested that improvements could be pursued within existing regimes as an interim measure.**

ON INFORMATION SHARING WITH GLOBAL AFFAIRS

- **CSIS and Global Affairs Canada have distinct mandates. We report to different Ministers and have our own legislative authorities. Both, however, perform vital functions and work together as appropriate, to protect Canadians and Canada's national interests.**

- **In the past, this sharing was authorized by specific provisions of the *Privacy Act,* which created challenges recognized by both partners and by SIRC in a review of our relationship.**

- **Now, Global Affairs Canada may share information with CSIS, both proactively and in response to requests, in accordance with the authorities in SCISA.**

- **This does not, however, in any way expand the Service's authority to collect information. It should also be noted that Global Affairs Canada is not collecting new information at our request; rather, Global Affairs Canada shares information gathered in exercising its responsibilities.**

- **To be clear, nothing in SCISA compels information sharing with CSIS. Global Affairs Canada is responsible for determining whether information may be shared.**

- **We have established an arrangement that governs the sharing of consular information to ensure any sharing is done in strict accordance with the law and Ministerial Direction.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

NATIONAL SECURITY FRAMEWORK

ISSUE: What is CSIS' role in the national security community? How does CSIS cooperate with domestic and international partners? Is the Service's operational cooperation with partners guided by frameworks or internal policies?

- **CSIS is dedicated to the safety of Canadians and the protection of Canada's national security – a mission that is clearly articulated in our legislation.**
- **Everything we do is anchored in the *CSIS Act*, which sets out the requirements for the conduct of our operations to investigate and respond to threats.**
- **We are, however, but one element of the broader national security community. This is recognized in our Act, which authorizes the Service to cooperate with domestic and foreign partners.**
- **In fulfilling our respective mandates, each partner has an essential role to play, but cooperation is critical at all phases – investigation, assessment and response.**

ON CSIS' ROLE IN NS FRAMEWORK:

- **In order to achieve our mission, to protect public safety, we investigate and respond to threats.**
- **The Service collects vital intelligence through a variety of methods, including the use of specific investigative techniques for which judicial authorization is required, and advises Government on threats to the security of Canada.**
- **CSIS collects information and intelligence to meet Government of Canada intelligence priorities. In so doing, we actively cooperate with partners, both to advance investigations and deconflict operations.**
- **In terms of our response, there are always a range of options to consider, often in consultation with partners.**
- **This can include a decision to investigate further, because we need to know more. Or, it could mean sharing information with partners to inform their lawful investigations or enforcement action (eg, citizenship or immigration decisions, Secure Air Travel Act).**

- **In some cases, it may be most appropriate for us to act directly to reduce threat-related activities.**

- **It is important to note that CSIS is not an enforcement agency. We do not have the authority to arrest or detain individuals, nor do we enforce laws or make administrative decisions.**

ON CSIS' COOPERATION WITH DOMESTIC PARTNERS:

- **Cooperation with domestic partners is critical to the success of the Service's lawful investigations and also serves to enhance advice provided to Government.**

- **Effective and responsible sharing of information between institutions is critical to our ability to protect Canadians.**

- **CSIS information may provide important insight for domestic partners, just as information lawfully collected by other federal departments may be relevant to active CSIS investigations.**

- **We have worked with domestic partners to develop tailored frameworks for cooperation to inform our operational cooperation, and continue to do so as our relationship and requirements evolve.**

- **Public safety is paramount, but CSIS must weigh the operational cost of publically releasing such information against the benefit of a potential prosecution or successful review of Government action.**

ON CSIS' COOPERATION WITH FOREIGN PARTNERS:

- **CSIS maintains a well-established network of relationships with partners abroad. These relationships are vital to CSIS operations.**

- **Without such collaboration, particularly from our Five-Eyes partners, Canada would suffer significant intelligence gaps.**

- **CSIS maintains more than 300 relationships with foreign agencies in over 155 countries, each authorized by the Minister.**

- **Through such relationships, CSIS advances its own investigations into threats to the security of Canada and gains a greater understanding of the scope and nature of threats.**

- **Ministerial Direction clearly states that in sharing information, CSIS must act in a manner that complies with Canada's laws and legal obligations and avoid any complicity in mistreatment by foreign entities.**

ON OPERATIONAL COOPERATION:

- **We have a regional presence across Canada and strong working relationships with partners to protect public safety, deconflict, investigate and respond to emergency situations including terrorist incidents.**
- **We cooperate in a multitude of ways, as appropriate. Sometimes this involves a multi-agency approach and other times it involves cooperation with a particular partner.**
- **For example, CSIS is an active participant in the National Security Joint Operations Centre and RCMP-led Integrated National Security Teams, to enhance our response to terrorist activities.**
- **Though real-time operational cooperation occurs, each partner must act within its own mandate.**
- **We routinely work with the RCMP in accordance with a framework for cooperation referred to as "One Vision."**
- **This framework recognizes our distinct mandates and authorities, and provides clear parameters for an effective working operational relationship.**
- **Of note, it was recently revised to reflect CSIS' threat reduction mandate and establishes an enhanced approach to operational cooperation, which shows the mature relationship between our two organizations.**
- **Though I can confirm that CSIS and RCMP engage regularly at both the executive and working levels to ensure decisions prioritize public safety and the broader public interest, I cannot discuss specific cases.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

THREAT REDUCTION MEASURES

ISSUE: Has CSIS engaged in TRA? How and against what threats? What are the safeguards and limitations on CSIS' TRA mandate? How has CSIS implemented this new mandate? How do you ensure that CSIS TRA does not impede RCMP investigations or reduce the likelihood of a prosecution?

- **Today's threats are fast, complex and dynamic, and threat actors are highly connected and mobile.**
- **From an operational perspective, recourse to a flexible range of response options is essential.**
- **In fulfilling its collection mandate, CSIS has developed unique expertise, capabilities and insight into threats to the security of Canada.**
- **In the past, both SIRC and Senate Committees contemplated a threat reduction mandate for the Service. In doing so, SIRC assessed that disruption may at times be necessary to protect Canadians. The Senate Committee reached a similar conclusion and suggested that this authority be clarified.**
- **The Service obtained its threat reduction authority with the passing of Bill C-51 in Summer 2015, which, amongst other things, amended the *CSIS Act*.**
- **Though new for Canada's intelligence service, Canada's closest democratic allies, including the US, Australia and the United Kingdom engage in threat reduction activity to varying degrees within their respective legal frameworks. Of note, none require the level of judicial review required in the *CSIS Act*.**
- **While we always consider the range of possible response options, CSIS has used its new threat reduction mandate to reduce threats to the security of Canada. This has always been done in consultation with domestic partners.**
- **It must be noted that SIRC has expressed its satisfaction with the rigorous governance framework that the Service has implemented to operationalize this new threat reduction mandate.**

- **Certain conduct is prohibited in all circumstances, including causing physical harm. These prohibitions mirror those applicable to law enforcement [as enshrined in the Criminal Code (s.25)].**
- **The Act also provides for a warrant regime, so that judicial authorization is required for any measure that would otherwise contravene the Charter or be contrary to Canadian law.**
- **In these circumstances, a Federal Court judge - not a CSIS employee - will determine whether the measure represents a reasonable limit on the right or freedom as is required**
- **I wish to clarify that threat reduction authorities do not equate to police powers. The power to arrest, detain, and enforce the law remain the purview of our law enforcement partners.**
- **The Act also contains new reporting requirements for CSIS and for the review by SIRC on the conduct of threat reduction.**

ON COOPERATION WITH PARTNERS

- **As you know, in today's global threat environment, national security is necessarily a team effort – which means that CSIS works with many domestic partners.**
- **We operate to protect Canada and Canadian interests, supporting one another while always respecting our distinct mandates.**
- **We have developed tailor-made frameworks with GAC, CSE and the RCMP, which set out clear direction on how we consult on threat reduction measures.**

ON WARRANTED MEASURES

- **Threat reduction measures must be reasonable and proportionate to the nature of the threat. In some cases, a warrant may be required.**
- **The *CSIS Act* clearly identifies when CSIS must seek a warrant to reduce a threat and what conditions must be satisfied for the Court to authorize certain measures.**
- **Should a warranted threat reduction measure be pursued, CSIS would be required to obtain Ministerial approval before seeking a warrant.**

- **I must note that the Service's threat reduction mandate is still relatively new and CSIS has taken an incremental approach to relying on this new authority to ensure its operationalization conforms with all policy and legislative requirements. As such, the Service has not yet required a warrant to proceed with a threat reduction measure, however, this should not be taken to mean that a warrant will not be required in the future.**

ON EXAMPLES OF NON-WARRANTED TRA:

- **It is possible to generally describe examples of non-warranted threat reduction measures. That said, caution must be exercised as each measure would need to be assessed on its own merits to determine the authorization required.**
- **Broadly speaking, examples of non-warranted threat reductions measures could include:**
  - **Employing human sources to provide a cautionary voice or counter-narrative;**
  - **Informing a family member or close friend of a prospective terrorist traveler of the individual's intentions, enabling them to intervene to dissuade the person from travelling;**
  - **Exposing CSIS' interest through interviews with the person, family members or associates in order to dissuade the person from taking certain actions;**
  - **Advising a hostile foreign intelligence operative, or informing the contacts of a known hostile foreign intelligence officer, that their affiliation is known to authorities;**
  - **Reporting social media accounts for violation of terms of use (hate speech/graphic violence) to allow Service providers to choose whether to remove the material.**

ON EXAMPLES OF WARRANTED TRA:

- **Though it is possible to generally describe examples of TRA requiring judicial authorization, caution must be exercised as each measure would be assessed on its own merits to determine the authorization required.**
- **Broadly speaking, examples of warranted threat reduction measures could include:**
  - **Intercepting and/or degrading equipment or weapons destined for terrorist or weapons-of-mass-destruction purposes;**
  - **Modifying or removing threat-related content on an extremist website; or**
  - **Disabling or altering personal electronics (computer, phone) used to support threat activities.**

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

GOING DARK

ISSUE: Is 'Going Dark' an issue/concern for the Service? What are the implications for 'Going Dark' for the Service? Why does CSIS require access to the personal and private details of Canadians?

- **The last 20 years have seen a rapid increase in the number of communications platforms, enabling near universal access to digital technology.**
- **At the same time, the diversity and complexity of communications technology has grown enormously.**
- **Communications services are moving away from traditional cable-and-wire infrastructure to virtual services, many of which originate from outside Canada. In other cases, a company may be headquartered off-shore or store data outside of Canada. Canadian laws governing communications service providers were not drafted for the borderless nature of telecommunications today.**
- **We are facing issues related to the maintenance of intercept capable networks, the widespread use of encryption and data retention requirements.**
- **This complex and rapidly evolving technological landscape presents significant challenges for CSIS in exercising our warranted authorities to collect information.**
- **Threat actors are also increasingly security aware and take advantage of digital tools to avoid detection.**
- **We refer to this issue as "going dark," meaning our warranted intercept coverage is lost or cannot be initiated. This can pose significant public safety risks.**

ON IMPACT OF "GOING DARK"

- **This issue has a significant and detrimental impact on our ability to fulfill our mandate. It also creates significant pressure on resources.**

- **To protect Canadians, Canada's national security and law enforcement agencies need to be able to exercise their lawful authorities, including court-issued warrants, and to do so in a timely manner.**
- **We are not talking about new or expanded authorities, rather the ability to exercise those that have long been in law.**
- **For the Service, this capability is necessary to identify and investigate threats to Canadians and the security of Canada.**
- **This technological landscape presents obstacles and poses complex challenges for CSIS in our work to investigate threats to Canadians and the security of Canada.**

ON RELATIONSHIP WITH COMMUNICATIONS SERVICE PROVIDERS AND PRIVACY

- **CSIS strives to maintain productive and cooperative relationships with communications service providers.**
- **Certainly, we are all navigating a difficult and changing landscape.**
- **Privacy and the ability to investigate criminal and national security threats are both important, and not mutually exclusive, objectives.**
- **Nor is there a requirement for communications service providers in Canada to ensure that their networks are capable of responding to court-authorized warrants to intercept communications.**

ON DATA RETENTION

- **Canada does not have standardized data retention requirements. The volume of electronic communications today creates pressure on providers to delete data in shorter timeframes.**
- **There is also no general requirement for providers to retain telecommunications data, such as the telephone numbers an individual has dialed, which may be needed as part of a lawful investigation.**
- **Once destroyed, vital communications information required to undertake lawful investigations may not be available.**

ON ENCRYPTION

- **Encryption is an important tool for safeguarding the privacy of Canadians and the security of personal, financial and trade data.**
- **However, the widespread availability of encryption technology also enables threat actors to conceal their communications and activities that threaten national security.**
- **The use of encryption creates delays and obstacles in the lawful investigation of threats to national security.**
- **Thus, while encryption is an important tool for security and privacy online, its increasing use also poses challenge for both CSIS and law enforcement agencies in exercising our warranted authorities.**

ON ACCESS TO BASIC SUBSCRIBER INFORMATION

- **As noted in the National Security Consultations, access to basic subscriber information is important for law enforcement and investigative agencies.**
- **Timely and effective access to basic subscriber information is important for CSIS in the course of our investigation of threats to the security of Canada, particularly in a modern technological environment.**
- **CSIS cannot comment further at this point as this policy work is ongoing.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

J

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

INTELLIGENCE AND EVIDENCE

ISSUE: Why is intelligence appearing in judicial proceedings? What are issues associated with the reliance on intelligence as evidence? Are there not existing authorities that protect the release of sensitive information?

- **As the Service's mandate is to investigate threats to the security of Canada and provide related advice to the Government of Canada, CSIS frequently shares threat-related information with other government departments.**
- **CSIS intelligence may therefore inform decisions made by our domestic partners, as they administer or enforce laws for which they are responsible.**
- **The result, however, is that CSIS intelligence is often drawn into public proceedings – civil, criminal or administrative.**
- **If released publicly, this information could compromise: intelligence operations, the safety of CSIS sources, CSIS capabilities and techniques, and Canada's relationships with foreign partners.**
- **It is therefore essential for the Service to protect sensitive national security information against public release using available legal tools, as appropriate.**

ON EXISTING AUTHORITIES TO PROTECT SENSITIVE INFORMATION

- **A number of regimes allow the Government to protect sensitive information from public release.**
- **For instance, Section 38 of the *Canada Evidence Act* provides for the protection of sensitive information when national security is at risk. The *CSIS Act* was also amended to provide greater certainty in relation to the protection of the identity of CSIS human sources.**
- **That said, when the Service's sensitive information must be publically released, CSIS must make a decision as to whether or not that information should be disclosed.**

- **In such instances, CSIS must weigh the operational cost of publically releasing such information against the benefit of a potential prosecution or successful review of Government action.**

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

K

Date: May 15, 2017
Classification: Unclassified
Agency: CSIS

Committee Note

BILL C-22 – AN ACT TO ESTABLISH THE NATIONAL SECURITY INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS

ISSUE: Does CSIS have resources dedicated to managing its relationship with the NSICOP? What type of work will the NSICOP generate for CSIS? What will the NSICOP be able to review? Will the NSICOP be able to review multi-department involvement in operations or investigations?

- **CSIS recognizes that effective accountability is key to maintaining Canadians' trust in Canada's national security community. The proposed Committee provides an opportunity for CSIS to demonstrate its commitment to contributing to these efforts.**

- **As written, the Bill provides the Committee with a broad mandate to review the full range of national security activities in all departments and agencies across the Government of Canada. This, of course, includes CSIS.**

- **Through its interaction with SIRC, the Service has gained significant experience with review. Building on this experience, we would certainly work to develop a similarly productive relationship with the Committee.**

- **It should be noted that Bill C-22 continues to be debated in Parliament, and the parameters around the creation of the NSICOP will be properly decided by Parliament.**

- **That said, CSIS will respect any review regime put in place, and looks forward to the opportunity to brief the Committee.**

ON ACCESS TO CLASSIFIED INFORMATION:

- **As is proposed, the Committee would be empowered to review the legislative, regulatory, policy, administrative and financial frameworks, including specific operations, of the Service.**

- **Given that members would have a Top Secret security clearance, the Committee could review classified information.**

- As such, the Committee would have access to all information held by the Service, with the exception of any exemptions defined in law.

ON AMENDMENTS TO EXEMPTIONS TO FULL ACCESS TO INFORMATION:

- I understand that questions of exemptions were actively debated at this committee and that associated provisions were subject to amendment at the report stage of the bill. As this is a question of public policy, it would be inappropriate for me to comment.

- CSIS would, of course, fully cooperate with the Committee and provide information relevant to its mandate.

ON THE PROTECTION OF CLASSIFIED INFORMATION:

- I understand the Committee would report to Parliament annually. It could also issue off-cycle reports on specific topics of interest.

- While much can be said publicly, if classified information were to be released, it could compromise: intelligence operations, the safety of CSIS employees and human sources, CSIS capabilities and techniques, and Canada's relationships with foreign partners.

- This may help explain why the Bill would allow the Prime Minister to advise the Committee to revise its reports to protect information if the disclosure would be injurious to national security, national defence or international relations.

- I would highlight our experience with SIRC in this regard. SIRC produces detailed classified reports. It also issues an Annual Report, which summarizes its reviews and findings. SIRC's Report is tabled in Parliament and, in my experience, certainly serves an important purpose.

ON CSIS RESOURCES DEDICATED TO REVIEW:

- **The Service has first-hand experience supporting review bodies. We have established a productive relationship with SIRC and this relationship continues evolve.**

- **We deliver verbal briefs, develop written submissions, produces documents and reviews public reports for national security injury and regularly liaises with the Committee and its staff.**

- **CSIS has resources dedicated to the external review of CSIS activities and will certainly dedicate the resources required to meet the Committee's expectations in a timely and efficient matter.**

ON CSIS' RELATIONSHIP WITH MULTIPLE REVIEW BODIES:

- **I understand the Bill encourages cooperation among all review bodies.**

- **These bodies will, however, remain autonomous institutions with distinct mandates.**

- **I cannot comment on the extent of the future relationship between the Committee and existing review bodies such as SIRC.**

- **I can, however, provide assurance that CSIS will, to the best of its ability, cooperate fully with all existing review bodies.**

- **As I have said, CSIS recognizes that effective accountability is key to maintaining Canadians' trust in the Government's national security activities.**

ON OVERSIGHT AND REVIEW

- **Review and oversight are often used interchangeably. That said, in our context, there is a distinction to be made in that oversight is often seen as suggesting either a role in operational decision-making, or some form of influence over operations as they are unfolding.**

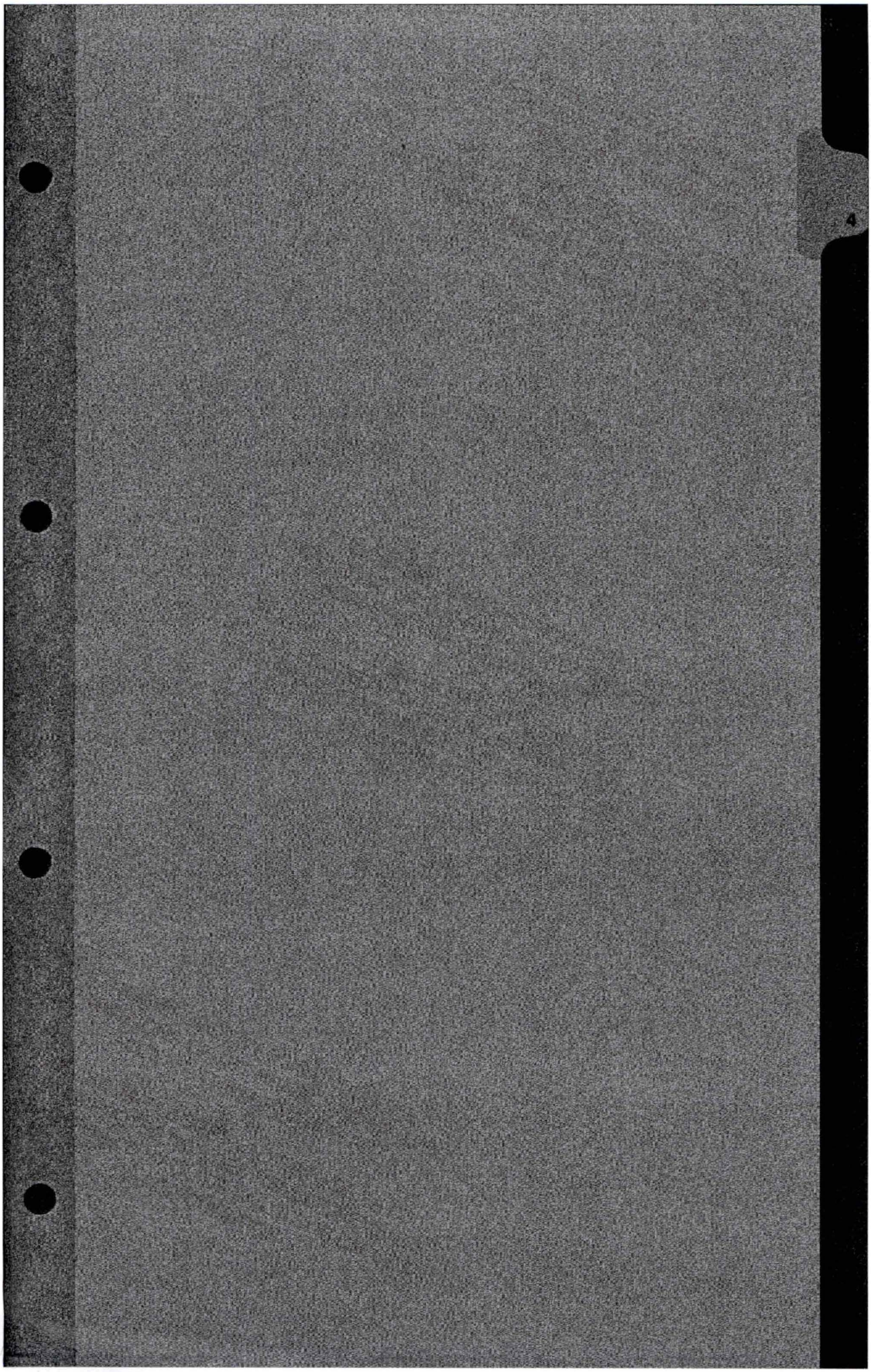
- **I understand the Bill would mandate the Committee to review, at its own discretion, many of the Service's programs, including specific operations. It is my understanding that the Committee would have access to a significant amount of information with which to do so.**

- **Such reviews would provide an opportunity to assure Parliament and the public that activities undertaken were lawful, reasonable and appropriate, and that the framework in place makes sense.**

- **My experience with SIRC is that though it is not involved in operational decision-making, its findings and recommendations have on many occasions, had a direct impact on CSIS policy and practice even in relation to ongoing activities.**

- **It is my understanding that the Bill does not provide an operational decision-making role for the Committee, but I do understand there may be interest in a very timely awareness of operations.**

- **As previously noted, the Committee will, however, be able to review operations and report on its review of these operations. As is the case with SIRC, CSIS will give serious consideration to any recommendation made by the Committee.**


4

News Summaries of Key Service Media Mentions
December 09, 2016 to May 10, 2017

Contents

Overview

Overall Service mentions were mostly related to the **metadata program**. Several new outlets reported that the Service had failed to mention the legal risks of the program.
In May, a number of reports focused on the government's release of the **Standing Committee on Public Safety and National Security's** review of national security policies.
CBC/Radio-Canada lead the way with three key reports on **Mobile Device Identifiers.**
Coverage of the ODAC/Metadata file remained strong, with the most substantive coverage appearing in the Globe and Mail.

(Mentions of Director are in bold)

Notable News articles

National Security Consultations

National security committee recommends watering down laws on terrorism peace bonds, propaganda
National Post, Stewart Bell, 2016 05 02
The committee of MPs reviewing Canada's national security policies has called on the Liberal government to loosen federal anti-terrorism laws concerning propaganda and advocacy of violence. The report by the Standing Committee on Public Safety and National Security, tabled on Tuesday, recommended narrowing the definitions of terrorism propaganda and what constitutes promoting terrorism. Currently, a judge can order the seizure of propaganda that "advocates or promotes the commission of terrorism in general." The MPs want to limit seizures to materials that counsel or instruct the commission of a specific terrorist offence. A section of the Criminal Code that makes it illegal to

advocate or promote "terrorism in general" should also be changed by removing the words "in general," according to the committee, chaired by Liberal MP Robert Oliphant. In a dissenting report, the Conservatives objected to the proposals, arguing that "to tackle radicalization via the Internet, promotion and advocacy of terrorism 'in general' needs to remain an offence under the Criminal Code."... The NDP said in its own supplementary opinion attached to the report that it wanted the law on advocating and promoting terrorism repealed altogether, saying it infringed on free expression and press freedom...Public Safety Minister Ralph Goodale's press secretary, Scott Bardsley, said the report would "inform decisions the government will make to confront new threats and challenges in the years ahead while at the same time safeguarding Canadians' Charter rights in a free and democratic society." Another recommendation could make it harder for police to obtain terrorism peace bonds. Preventive peace bonds can now be sought against a suspect if a police officer "believes on reasonable grounds that a terrorist activity may be carried out." The report has suggested replacing "may be" with "on the balance of probabilities.".. Under the committee's proposal, before a peace bond could be issued prosecutors would have to prove it was more probable than not that a terrorism offence would occur, said University of Ottawa law professor Craig Forcese. "That's a pretty significant burden and I don't see how peace bonds would prove a very useful tool going forward," said the national security law expert, who testified before the committee last November. He welcomed the recommendations to reign in the propaganda and promotion laws, which he said were ambiguous and raised free speech issues.

Terrorisme: Ottawa va restreindre les pouvoirs de ses espions

Le Devoir, Hélène Buzzetti, 2017 05 03

James Bond pourrait devoir remballer sa quincaillerie. Du moins, c'est ce que propose le Comité parlementaire sur la sécurité publique et nationale, qui suggère à Justin Trudeau une quarantaine de mesures pour mieux encadrer les pouvoirs antiterroristes canadiens, notamment ceux des espions. La Loi antiterroriste adoptée par le précédent gouvernement conservateur en 2015, peu avant l'élection, avait suscité une vague d'indignation. Le C-51 octroyait au Service canadien du renseignement de sécurité (SCRS) le pouvoir -- autrefois réservé aux policiers -- de " perturber " les activités de personnes sous surveillance. Il élargissait aussi le nombre de personnes pouvant se voir interdites de vol. En campagne électorale, M. Trudeau a promis de revoir certains éléments de cette loi. Un comité parlementaire (à majorité libérale) s'est penché sur la question, et c'est le fruit de sa réflexion qui a été dévoilé mardi. Le comité suggère de limiter le pouvoir de perturbation du SCRS en exigeant que chaque perturbation soit avalisée par un juge. À l'heure actuelle, seules celles contraires à la Charte des droits et libertés doivent l'être. Le comité propose d'interdire les perturbations contraires à la Charte. Celles qui contreviendraient à une loi autre devraient être entérinées par le ministre de la Sécurité publique. Selon le directeur du SCRS, le pouvoir de perturbation a été utilisé une vingtaine de fois et jamais un mandat n'a été nécessaire. " Il arrive parfois que le SCRS doive intervenir promptement sur la base d'informations qu'il a, mais nous disons qu'il ne devrait jamais agir en contravention de la Charte. Il ne devrait pas y avoir d'exception ", a expliqué le président du comité, le libéral Rob Oliphant. Le comité suggère par ailleurs que le SCRS " épuise tous les autres moyens à sa disposition [...] avant d'exercer ses pouvoirs de perturbation ". C'est que ce pouvoir -- que les policiers ont eu de tout temps, par exemple en participant à une transaction de drogue pour la faire dérailler -- prend une tout autre dimension lorsqu'octroyé à un service de renseignement. Car ce dernier, contrairement à un corps policier, n'a pas de pouvoir d'arrestation. Les interventions du SCRS ne conduisent pas au dépôt d'accusations et à un procès au cours duquel la légalité desdites interventions pourrait être contestée. Le ministre de la Sécurité publique, Ralph Goodale, a indiqué qu'il entendait déposer un projet de loi d'ici l'été. Sans promettre de mettre en oeuvre toutes les recommandations du comité, il a souligné que celles-ci se rapprochaient beaucoup de ce qu'il avait en tête. " En général, ce que nous avons entendu lors des consultations publiques et ce que propose le comité vont dans la même direction que notre plateforme électorale. "

Ottawa has even more reason to fix security law
Toronto Star editorial, 2017 04 17

An editorial states "The government has run out of reasons for delay on Bill C-51. It should move as quickly as possible to fix this bad law. So it turns out that this country's spy agency, the Canadian Security Intelligence Service (CSIS), may not actually need the additional powers the Harper Conservatives gave it back in 2015. That's the gist of an eye-opening report from Ottawa by the Star's Alex Boutilier and Tonda McCharles. They report that CSIS has suspended use of the most controversial powers to disrupt threats of terrorism that were contained in the Conservatives' Anti-Terrorism Act, also known as Bill C-51... This could be simple political caution. But it has some security experts wondering whether CSIS truly needed the controversial powers in the first place. It may be able to carry out its mission of preventing threats to national security without having to go to a judge for authorization to take exceptional measures. If so, it makes it all the more urgent for the government to finally fulfill its campaign promise to change Bill C-51.

Goodale plans spring legislation to revamp controversial anti terror law C 51
Canadian Press, Jim Bronskill, 2017 03 22
Ottawa - The federal Liberals plan to introduce legislation this spring to revamp the Conservative anti-terrorism bill known as C-51, the public safety minister says. The package could include other measures that flow from the government's recently concluded national security consultation, Ralph Goodale said in an interview. The Liberals promised during the last election to repeal ``problematic elements" of omnibus security legislation ushered in by the previous Conservative government after a gunman stormed Parliament Hill. C-51 gave the Canadian Security Intelligence Service explicit powers to disrupt terrorist threats, not just gather information about them. It also created a new offence of promoting the commission of terrorist offences and broadened the government's no-fly list powers. The Trudeau government has committed to ensuring all CSIS warrants respect the Charter of Rights and Freedoms, to preserving legitimate protest and advocacy and to defining terrorist propaganda more clearly. It has also pledged that appeals by Canadians on the no-fly list will be subject to mandatory review. The Liberals have faced persistent pressure from the NDP and civil libertarians to move quickly on the changes, but the government opted to consult widely and take its time. Tens of thousands of people took part in the national security consultation, and there was ``a tremendous amount of consensus" on the Liberal platform promises, Goodale said. Two other commitments are nearing fruition _ a special committee of parliamentarians to oversee intelligence activities and a federal office that will focus on national counter-radicalization efforts. MPs who studied a bill to create the committee of parliamentarians made several amendments to bolster its powers. Opposition parties expressed dismay when the government recently nixed some of the changes, including the authority to subpoena witnesses and documents. Critics say the prime minister will wield too much power over the committee and that it will lack the tools to get to the bottom of intelligence scandals and failures. Goodale denies the bill has been gutted, arguing it is only prudent to place some limitations on the committee's powers given the extreme sensitivity of the files it will probe.

Metadata Program

RCMP created metadata-crunching tool to glean criminal intelligence
Canadian Press, Jim Bronskill, 2017 05 08
The RCMP created, then suddenly abandoned, a tool to crunch electronic message trails gathered during criminal investigations – a previously unknown foray into the controversial realm of big-data analysis. The Mounties' national intelligence co-ordination centre was operating the Telecommunications Analytical Platform, as the tool was known, as recently as mid-November, say internal RCMP notes obtained by The Canadian Press through the Access to Information Act. "The TAP is a platform that regroups copies of certain telecommunications metadata, which are lawfully collected by the RCMP and other Canadian police services in the course of criminal investigations," the RCMP notes say. Metadata is information associated with communications, but does not include the content of actual emails or phone calls. Still, privacy advocates say it can reveal much about a person and should be subject to strict handling procedures. The RCMP tool analyzes metadata from concluded investigations only, such as phone numbers, associated crime types, source links to police records management systems and the geographical region where the metadata was recorded, the notes add. The tool was a "proof of concept" that turned out to be unsuccessful and "therefore the project was ended," said Cpl. Annie Delisle, an RCMP spokeswoman. "No data was retained." News of the RCMP information-sifting tool's apparently brief existence follows a furor over the Canadian Security Intelligence Service's data analysis centre. In early November, Federal Court Justice Simon Noel said CSIS violated the law by keeping electronic data about people who were not actually under investigation. His sharply worded ruling said the spy service should not have retained the information because it was not directly related to threats to the security of Canada.

Public safety ministers weren't briefed on legal risks of CSIS metadata retention
iPolitics.ca, Amanda Connolly, 2017 03 18
Ottawa - The documents used to brief five successive public safety ministers on a CSIS metadata retention program failed to mention the legal risks of that program, which was ruled illegal last year. Documents obtained by iPolitics under access to information laws show that beginning in 2006, public safety ministers were given broad overviews of the existence of the Operational Data Analysis Centre, but none of the documents raised the issue of whether such a program could have potential legal implications. National security experts say that the documents suggest ministers were "kept in the dark" by the spy agency and that changes should be made to how ministers are briefed in the future. The Federal Court ruled in November 2016 that the metadata collected -- such as call logs -- was not directly related to threats to the security of Canada, and noted the spy agency had breached its duty to inform the court of the program, given that the metadata was collected using judicial warrants issued over a decade, from 2006 until the program was suspended last fall in response to the ruling. CSIS officials have so far declined to say how many Canadians may have had their privacy breached, but it would be a greater number than those who were the subject of warrants given that the metadata included information about things such as to whom a subject of a warrant placed texts or phone calls during the time they were under surveillance.

CSIS failed to give updates on data spying: watchdog
Globe and Mail, Colin Freeze, 2017 03 17
Toronto - When intelligence-agency analysts reported to federal privacy officials about their budding data-mining efforts, they argued these activities presented only a minimal risk to Canadians' confidential data. But the Canadian Security Intelligence Service also conceded this might very well change. Because the scale and scope of the early efforts would surely snowball over time, they vowed to give formal, written updates to the Office of the Privacy Commissioner of Canada. Yet, this has not happened in the seven years since CSIS submitted its first Privacy Impact Assessment (PIA), a 2010 document that appears to have predated a period of significantly steppedup data spying. "It's the only PIA that we have received," Privacy Commissioner Daniel Therrien said in an interview with The Globe and Mail on Thursday. In 2006, CSIS had promised its minister in a written memo that it would voluntarily brief the judges about ODAC. By 2015, a watchdog body released a report to Parliament urging CSIS to come clean with the judges. But the spy service initially resisted the advice, saying that it "was both inappropriate and unwarranted. Following the Federal Court ruling, he added, CSIS Director **Michel Coulombe** invited his office to renew the dialogue. The conversation is now ongoing. The Globe recently reported that, in 2012, CSIS analysts circulated a PowerPoint where they mulled how much could they enhance the efficacy of ODAC by obtaining "bulk datasets."

CSIS to resume data-mining practices
Globe and Mail, Colin Freeze, 2017 03 16
Toronto - A mysterious federal intelligence centre is back in the business of warehousing telecommunications trails that have been covertly captured in Canada. This is because the legal issues with the Operational Data Analysis Centre have been mostly fixed, according to the Canadian Security Intelligence Service. News of this development comes six months after the Federal Court of Canada made headlines for challenging CSIS's credibility and outing ODAC by declaring aspects of its datamining operations illegal. "As of March, 2017, CSIS has implemented new retention practices for information," Tahera Mufti, a CSIS spokeswoman, said in an e- mail to The Globe and Mail. These fixes should pass muster with judges, she said, thus "allowing ODAC to recommence its analysis" of once-contentious data. Such programs are "vital to the service's national-security investigations," she added.

CSIS reneged on pledge to brief judges about secret data centre
Globe and Mail, Colin Freeze, 2017 03 15
Toronto - When Canadian intelligence analysts launched a program to warehouse telecommunications data, the top spymaster of his time reassured his minister in a memo that judges would be told about it "at an appropriate juncture." Over the next decade, that juncture never materialized. This omission set the stage for a scathing court ruling last fall that shook the credibility of the Canadian Security Intelligence Service. The 2006 CSIS memo recently acquired by The Globe and Mail under access to information laws raises questions about whether Canada's spy service is revealing enough about its intelligence operations to its political bosses and the judges who oversee its wiretap warrants. In the aftermath, CSIS director **Michel Coulombe** apologized for the omissions and released a list of occasions on which the agency mentioned ODAC to cabinet ministers and intelligence watchdogs. Yet some of the communications mentioned by Mr. Coulombe, who this week announced he will retire, still glossed over the legal implications of the data analysis program.

CSIS saw 'no high privacy risks' with metadata crunching now under fire: docs
Canadian Press, Jim Bronskill, 2017 02 27
Ottawa - The national spy service saw little risk to the personal privacy of Canadians in a self-penned evaluation of its secret data- crunching centre _ a shadowy program now at the centre of intense controversy, newly released documents show. The Canadian Security Intelligence Service centre touched off a firestorm late last year when a judge said CSIS had broken the law by keeping and analyzing the digital metadata of innocent people. The ruling also prompted debate about what future role the spy service should have _ if any _ in using such potentially revealing information in its work. But a privacy impact assessment of the Operational Data Analysis Centre prepared in August 2010 _ and secret until now _ offered little hint of such concerns. ``The assessment process has identified no high privacy risks," says the 62-page CSIS reportThe Canadian Press obtained a heavily censored version of the classified CSIS document through an Access to Information request. CSIS director **Michel Coulombe** testified that he hoped the spy service would be in a position within about six months to decide what to do with the associated metadata collected over the 10-year period. The 2010 privacy impact assessment said that while CSIS believes in openness and transparency, due to the ``extreme sensitivity" of the data analysis centre's work, ``it is not possible to communicate about that work to the public."

Goodale orders CSIS program review
Toronto Star, Alex Boutilier, 2017 02 03
Toronto - Public Safety Minister Ralph Goodale has ordered a review into a CSIS metadata program that illegally stored data on innocent Canadians for almost a decade. Goodale said Thursday that he and Justice Minister Judy Wilson-Raybould are examining the circumstances that led CSIS and the Department of Justice to conclude the spy agency could collect and store data on "non-threat" individuals indefinitely. The review was requested after a Federal Court ruled the practice was illegal late last year, Goodale's office said Thursday night. "The work that CSIS did was all based upon the considered legal opinions that they had from the Department of Justice," Goodale told the Star in an interview. "So it's important to make sure that, from the operational side, which is Public Safety, but also the policy side, which is the Department of Justice, that we get this right." In a **related report**, Boutilier points out that CSIS says they don't know how many Canadians were caught up in an illegal metadata program that operated for almost a decade. In documents tabled in Parliament this week, CSIS told MPs they are "unable" to determine how many innocent people had their data stored and analyzed at the agency's Operational Data Analysis Centre. In a November press conference, CSIS Director **Michel Coulombe** said the agency had no records to justify keeping the ODAC's operations from the Federal Court. "I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed," Coulombe told reporters.

Mobile Defice Identifiers/IMSI

Spies' use of cellphone surveillance technology suspended in January, pending review
CBC News/Matthew Braga and Dave Seglins, 2017 05 04
Canada's spy agency suspended its use of a controversial cellphone surveillance technology in January and placed the investigative technique under review, CBC News has learned. The Canadian Security Intelligence Service (CSIS) confirmed it has used the cellphone identification and tracking technology in recent years, both with and without a warrant. The devices are often colloquially referred to as Stingrays

after a well-known brand, but are also known as IMSI catchers, mobile device identifiers (MDIs) and cell-site simulators. They collect information about cellphones in a given area by pretending to be legitimate cell towers, and are used by both intelligence agencies and police to investigate crimes or national security threats. "The policy and procedures for use of MDI devices to support CSIS operations is under internal review," agency spokesperson Tahera Mufti wrote in an email. "The use of the devices was suspended until the recommendations of the review are completed." CSIS declined to comment on what prompted the review, what internal recommendations have been made or why the agency decided to suspend the use of the technology for months. After a decade of silence, the RCMP revealed last month that it has also been using IMSI catcher technology, prompting other police agencies across the country to make similar disclosures to CBC News. Unlike the RCMP, CSIS refused to say how frequently it used IMSI catchers, citing "operational security reasons." However, the agency did state that, like the RCMP, "the equipment currently used by CSIS is not capable of intercepting content."

Surveillance électronique à Ottawa - La GRC et le SCRS clament leur innocence
Radio-Canada, 2017 04 04
Quelqu'un écoute peut-être les conversations téléphoniques au centre-ville d'Ottawa, mais ce n'est pas une agence gouvernementale canadienne. Une enquête est maintenant ouverte pour découvrir l'identité des indiscrets. Radio-Canada a révélé lundi soir que des " intercepteurs d'IMSI " avaient été en fonction au centre-ville d'Ottawa, en particulier en décembre et janvier derniers. Ces intercepteurs imitent le fonctionnement d'une antenne de téléphone cellulaire. Les téléphones se trouvant dans un rayon de 500 mètres s'y connectent et révèlent leur identité. Les intercepteurs d'IMSI peuvent même parfois capter le contenu d'un texto ou d'une conversation téléphonique. Compte tenu des lieux de détection de ces appareils par Radio-Canada, les zones couvertes englobent la colline du Parlement, les bureaux de tous les médias couvrant la politique fédérale, la Défense nationale, l'édifice du premier ministre canadien ainsi que les ambassades américaine et israélienne. Le ministre de la Sécurité publique, Ralph Goodale, a indiqué avoir contacté le directeur du Service canadien du renseignement de sécurité (SCRS), Michel Coulombe, et le commissaire de la Gendarmerie royale du Canada (GRC), Bob Paulson, pour savoir ce qu'il en retourne. " Ils m'ont confirmé deux choses. D'abord, bien que nous ne commentions pas en temps réel les questions opérationnelles, les activités mentionnées dans le reportage de lundi soir n'impliquent pas une agence canadienne telle que la GRC ou le SCRS. " M. Goodale est catégorique : si une telle activité de surveillance était menée par une agence canadienne, elle aurait été d'abord approuvée par un juge. "

Someone is spying on cellphones in the nation's capital
CBC News, 2017 04 03
A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill. The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime. The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone - the International Mobile Subscriber Identity, or IMSI. That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls. We wanted to know more about who might be using the IMSI catcher or catchers that we detected, so we asked the U.S. supplier of the CryptoPhone to analyze the alerts we were getting. ESD America specializes in counterintelligence and its clients include U.S. Homeland Security. "Consistently you've been seeing IMSI catcher activity, definitely," said CEO and co-founder Les Goldsmith, when we took our results to the company's Las Vegas office. Based on the configurations suggested by CBC's results, he believes the IMSI catchers detected in Ottawa could be foreign made. "We're seeing more IMSI catchers with different configurations and we can build a signature. So we're seeing IMSI catchers that are more likely Chinese, Russian, Israeli and so forth," he said. We also showed our results to an expert in Canadian security. He knows a lot about IMSI catchers

and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work. The expert found the results of our investigation disturbing. "That an MP or a person who works on Parliament Hill could be exposed, that they could be a victim of this type of attack- it undermines our sovereignty," he said. Our security expert suggested the IMSI catchers we saw might be the work of a domestic agency, like Canada's electronic spy agency, the Communication Security Establishment. "One possibility is that the Communications Security Establishment has been mandated to monitor the network for protection purposes, in a defensive way," he said. CSE said it's not allowed to do that. The Department of National Defence said it had no knowledge of IMSI catchers being used on the dates we saw activity. The Department of Public Safety, the Ottawa Police Service, the RCMP and CSIS all gave similar responses: They don't discuss specific investigative techniques but they do follow the law, respect the Charter of Rights and Freedoms and adhere to the appropriate judicial processes.

Russian Interference

Call Russia's Freeland smear out for the lie it is: Clement

iPolitics, Amanda Connolly, 2017 03 07

Ottawa - Conservative public safety critic Tony Clement said today journalists and politicians of all stripes have a responsibility to call out Russian propaganda smearing Foreign Affairs Minister Chrystia Freeland for the lie it is. Over the past week, Russian propaganda websites have published content claiming that Freeland's maternal grandfather was a Nazi collaborator. Several Canadian outlets, including the Globe and Mail and Vice, have said they received similar allegations from individuals within the Russian embassy and worked to trace the smear back to demonstrate that the claim is not actually true. When asked whether he was concerned about Russia targeting a Canadian official in a smear campaign, Clement said in a scrum before question period that this is exactly what the world has come to expect from the Russian government and that Canadians should not let themselves be distracted. "You know what? The Russian government are a bunch of liars. They do this all the time. They've been doing it for 80 years under the Soviet Union and now under the new Soviet Union that is Putin's Russia," he said. "You have a responsibility, we all have a responsibility to expose these lies for what they are — state propaganda policy by Putin's Russia to confuse, to lie, to make sure that we're all fighting one another." As iPolitics reported last fall, Canadian officials are bracing for a smear campaign by pro-Russian agents opposed to Western deterrence efforts in Eastern Europe, particularly in Latvia and the Baltics. Defence Minister Harjit Sajjan and Canadian Forces intelligence chief Stephen Burt warned that Canadians should expect to see an increase in allegations attacking the credibility of Canadian soldiers and activities, and be prepared to ignore them. Freeland also echoed those comments when asked about the current smear campaign against her during a press conference on Monday in which she and Sajjan announced the renewal of Operation Unifier, Canada's training mission in Ukraine, for another two years.

Freeland warns Canadians to beware of Russian disinformation

Globe and Mail, Robert Fife, 2017 03 07

Ottawa - Foreign Affairs Minister Chrystia Freeland, who is being targeted by allegations in pro-Moscow websites that her maternal Ukrainian grandfather was a Nazi collaborator, warned Monday that Canada should expect to be the focus of Russian disinformation campaigns similar to what is happening in Europe and the United States. Russia has shown its displeasure at Ms. Freeland's promotion to Foreign Affairs Minister by maintaining a travel ban against her as well as critical articles in state-owned media. Recently a number of stories have appeared in pro-Putin regime websites, calling Ms. Freeland "Canada's

fiercely anti-Russian Foreign Affairs Minister" and alleging her grandfather, Michael Chomiak, was a Nazi propagandist in Poland. "I don't think it's a secret. American officials have publicly said, and even [German Chancellor] Angela Merkel has publicly said, that there were efforts on the Russian side to destabilize Western democracies, and I think it shouldn't come as a surprise if these same efforts were used against Canada," Ms. Freeland told reporters when asked about the articles. "I think that Canadians and indeed other western countries should be prepared for similar efforts to be directed at them." Ms. Freeland is a strong advocate of Ukrainian independence and a tough critic of Russia's annexation of Crimea. A former financial journalist who worked in Moscow, she was blacklisted in 2014 along with 12 other Canadians for advocating western sanctions against Russia. Without commenting on the allegations against Ms. Freeland's grandfather, Public Safety Minister Ralph Goodale told reporters Canadian politicians need to be alert to Russian disinformation tactics, including efforts to hack into computer systems as the Russians did with the Democratic Party. "The situation is obviously one where we need to be alert. And that is why the Prime Minister has, among other things, encouraged a complete re-examination of our cyber security systems," Mr. Goodale said. "And that is why we're offering the services of the [Communications] Security Establishment to provide advice to political parties about whether or not they are as secure as they need to be." A spokesman for the Russian embassy in Ottawa, Kirill Kalinin, said the Putin government did not have anything to do with the stories about Ms. Freeland's grandfather.

Alleged surveillance of journalists/protesters

Canada's spy agency was watching Standing Rock
Vice News Canada, Hilary Beaumont, 2017 03 16
Two secret reports on Standing Rock obtained by VICE News show the Canadian spy agency has been monitoring the protest camps and acts of pipeline sabotage in the U.S. and believes they have Canadian implications. The documents shed light on how Canada's security apparatus viewed the massive mobilization of opposition to the $3-8-billion Dakota Access Pipeline, which the protesters said will destroy sacred sites of the Standing Rock Sioux Tribe, and threaten their water supply. In one document dated Sept 22, 2016, the Canadian Security Intelligence Service (CSIS) states "there is strong Canadian Aboriginal support for the Standing Rock Sioux Tribe as many see similarities to their own struggles against proposed pipeline construction in Canada (Northern Gateway, Pacific Trails, Energy East, etc.)." The intelligence service also writes that there is a Canadian dimension to the "co-ordinated sabotage in support of Standing Rock."

'This is a big deal for us,' talks continue over plans for Hill media security screening
The Hill Times, Laura Ryckewaert, 2017 03 28
Ottawa - Talks are ongoing between the Parliamentary Press Gallery and House of Commons officials and concerns remain over a proposed security- screening process for new reporters. "We're still in a fact-finding and a discussion stage," said Tonda MacCharles, the new president of the Parliamentary Press Gallery and a Toronto Star reporter. "This is a big deal for us," she said. "We are very concerned that bit-by-bit access is overly controlled and overly rigid. You can have the illusion of security on Parliament. You can think you've screened people for a criminal record. Does that make you safer? I think that this is

really a big project for the gallery this year." Ms. MacCharles added: "We're trying to determine what are the practices in other legislatures, and to what extent this is a proposal that is either well underway and already fixed, or is it something where there is still a bit of negotiating room." Along with Ms. MacCharles, the current gallery executive includes: Radio-Canada's Philippe-Vincent Foisy as vice-president; CBC's Elizabeth Thompson as treasurer; and Huffington Post Quebec's Catherine Lévesque as secretary. The directors are freelancer Gerhard Braune, iPolitics' Amanda Connolly, Le Devoir's Manon Cornellier (past-president), The Canadian Press' Kristy Kirkup, CBC's Chris Rands, and The Globe and Mail's Michelle Zilio. The gallery first received notice of the House's plans to introduce a new security-screening process for journalists to access Parliament Hill last summer. A briefing on the plan-which originally involved the Canadian Security Intelligence Service (CSIS)-with House and security officials took place in November and led to talks to amend and clarify the process.

Parliamentary press gallery pushes back against plan to fingerprint, screen reporters
CBC.CA, Kathleen Harris, 2017 02 25
Ottawa - The parliamentary press gallery is challenging a plan to impose RCMP security screening measures on new members, including fingerprinting for criminal record checks. The gallery, which marked its 150th year as an organization in 2016, formally opposed in principle the proposal from a House of Commons administrative committee during an annual meeting at the National Press Theatre today. The gallery's executive will seek answers on why the screening is necessary, what threshold for criminal background could potentially bar access to Parliament Hill, and why fingerprinting is necessary. The initial proposal suggested that Canada's spy agency, CSIS, be involved in the screening process, but that was dropped after resistance from the gallery executive. Members raised concerns the new measures could infringe on freedom of the press. Press gallery president Tonda MacCharles, a veteran reporter with the Toronto Star, said journalists have been sent to cover Parliament Hill by employers who have entrusted them to do the job.

Chinese Takeover/journalists

Des journalistes chinois dans la ligne de mire du SCRS
La Presse, Joël-Denis Bellavance, 2017 05 01
Le Service canadien du renseignement de sécurité (SCRS) a traqué des journalistes chinois en poste à Ottawa au cours des dernières années parce qu'il les soupçonnaient de se livrer à des activités d'espionnage aux dépens du gouvernement canadien ou d'organisations qui étaient d'un grand intérêt pour la Chine. Une enquête de La Presse a permis d'obtenir des informations inédites sur les activités de contre-espionnage menées par le SCRS dans le but de tenir à l'œil les journalistes chinois affectés à la couverture de la politique nationale. Selon nos informations, le SCRS s'est particulièrement intéressé au fil des ans à des journalistes du Quotidien du peuple et de l'agence chinoise Xinhua, deux médias perçus par les services secrets canadiens - et par plusieurs hauts fonctionnaires canadiens - comme des agents qui obéissent aux diktats du gouvernement communiste de Pékin. Les journalistes qui travaillent pour ces médias à Ottawa sont également membres de la Tribune de la presse parlementaire. Ils jouissent ainsi d'un accès privilégié aux événements organisés par le bureau du premier ministre et les divers ministères ou agences gouvernementales. « Dans les hautes sphères du gouvernement canadien, tout le monde sait pertinemment que les employés de ces médias ont un rôle bien précis à Ottawa : colliger des informations stratégiques qui intéressent le gouvernement chinois. « Je ne peux donner de détails sur l'objet des enquêtes, mais la Loi sur le SCRS est très claire : le SCRS ne peut enquêter que sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du

Canada », a indiqué Dan Brien, directeur des communications du ministre de la Sécurité publique Ralph Goodale, en réaction aux informations obtenues par La Presse. « Comme nous l'avons indiqué précédemment, les journalistes ne sont pas l'objet des enquêtes pour déterminer leurs sources. Ainsi, le SCRS ne pourrait ouvrir une enquête sur un journaliste que s'il existe suffisamment d'informations qui donnent à penser que ce dernier participe à des activités qui constituent une menace pour la sécurité nationale. Le SCRS s'acquitte de ses responsabilités avec une grande rigueur », a-t-il ajouté. M. Brien a affirmé que pour le SCRS, « la liberté de la presse est une valeur canadienne fondamentale ».

Liberal green light for Chinese takeover deal a turning point for Canada: experts
Globe and Mail, Steven Chase, 2017 03 29
Ottawa - The Trudeau government's decision to approve a Chinese takeover deal originally rejected in 2015 as too risky for national security marks a significant shift in Canada's approach to Beijing, and may encourage China to invest more heavily in cutting-edge Canadian firms that might have been considered off-limits before, experts say. Hong Kong-based O-Net Technology Group announced this week that Prime Minister Justin Trudeau's cabinet had given it the green light to purchase ITF Technologies of Montreal, a leader in fibre-laser technology. Applications for such technology include directed-energy weapons. This represents a complete reversal in Ottawa's attitude to this deal, which the Harper government in 2015 blocked after national security agencies warned them the transaction would undermine a technological edge that Western militaries have over China. " This change of heart on the deal only came to light this week because O-Net announced it in a filing with the Hong Kong Stock Exchange. O-Net said it was informed March 17 the transaction could proceed. Ward Elcock, a former director of the Canadian Security Intelligence Service, said he's not familiar with the target company - ITF - and whether its technology is cutting edge. He also noted he had no way of verifying the 2015 national security assessment that warned the transaction would deliver a significant benefit for Beijing. "If the technology is as sensitive as the report you mentioned in [The Globe and Mail] would suggest, then I would have to say that it is not something I would have recommended be approved," Mr. Elcock said in an interview. He was the director of CSIS between 1994 and 2004.

Ottawa accused of appeasing Chinese with second review of takeover
Globe and Mail, Steven Chase, 2017 01 24
Ottawa - The Trudeau government is being accused of bowing to Beijing by cancelling a cabinet order to break up a Chinese takeover of a Montreal hightech firm despite warnings from national security agencies that the deal would undermine a technological edge Western militaries have over China. The Liberal government recently set aside a Harper government decision from 2015 that would have required Hong Kong-based O-Net Communications to abandon its purchase of Montreal's ITF Technologies. Ottawa then ordered a fresh review. But the change in direction has raised questions from opposition parties, experts and a former spy chief. The Globe and Mail revealed this week that, in 2015, both the Canadian Security Intelligence Service and the Department of National Defence issued warnings against allowing the sale. These assessments prompted the Conservative government in July, 2015, to order a breakup of the transaction on the grounds it would be injurious to national security - a move that China's O- Net immediately appealed to the Federal Court. "If the technology is transferred, China would be able to domestically produce advanced military laser technology to Western standards sooner than would otherwise be the case, which diminishes Canadian and allied military advantages," a national- security assessment prepared for cabinet by the Department of National Defence and CSIS said in 2015. Instead,

the Liberals in November, 2016, granted O-Net a second chance to win national security approval for the transaction and Ottawa began a new review of the deal.

Former CSIS directors question merits of China extradition deal
Globe and Mail, Staff reporters, 2017 03 29
Ottawa - Two former Canadian spymasters are questioning the wisdom of pursuing an extradition treaty with China, an undertaking the Liberal government announced shortly after Prime Minister Justin Trudeau made his first official visit to the Asian power. Australia paused efforts to enact a similar accord with China this week in the face of opposition, even from within Prime Minister Malcolm Turnbull's own party. China immediately appealed to the Trudeau government not to follow Canberra's lead. A cross Pacific extradition treaty "is for mutual benefit. It deserves serious consideration," Foreign Ministry spokeswoman Hua Chunying said Tuesday. "Such a treaty will help the two countries in having an institutional guarantee in combatting transnational crimes," she added. But Ward Elcock, who served as director of the Canadian Security Intelligence Service from 1994 to 2004, said Tuesday he doesn't think Canada should ink an extradition deal with China. Long demanded by China, an extradition treaty would commit Canada to transferring fugitive Chinese officials to a country known for biased courts and harsh interrogation methods - and where the death penalty can be imposed even for non-violent crimes. He raised concerns about whether Canada would be able to obtain sufficient guarantees that individuals shipped back to China would be treated properly.

Others

Canada's top spy agencies work out deal on 'threat disruption' operations
Toronto Star, Tonda MacCharles and Alex Boutilier, 2017 04 14
Canada's two most powerful intelligence agencies have crafted a formal deal to cooperate on using controversial powers to disrupt domestic threats to the country's security, the Star has learned. Documents obtained by the Star show the spy agency Canadian Security Intelligence Service (CSIS) and the electronic signals-gathering agency Communications Security Establishment (CSE) signed an agreement in July 2016 on how CSE will assist with "threat reduction" activities. For example, if CSIS were to jam electronic communications, thwart a suspected terrorist's travel plans or financing efforts, or crash a group's or individual's website, it would notify CSE it was intending to act. The power to actively intervene to disrupt threats to Canadian national security, rather than simply collect information on them, was granted to CSIS in the previous Conservative government's contentious anti-terrorism law, Bill C-51. The legislation allows CSIS to actively disrupt perceived threats to national security, with few limits to the power except obtaining a warrant. The agreement with CSE allows for the combination of CSIS's expertise in human intelligence and field work with the technical sophistication of Canada's premier electronic intelligence agency. Toronto Star (Alex Boutilier & Tonda MacCharles)

Canadian spies must be ready to operate abroad: CSIS annual report
iPolitics.ca, Amanda Connolly, 2017 03 01
Ottawa - The global security climate is not getting better any time soon and Canadian spies need to be prepared to investigate threats beyond Canada's borders. That's the driving message behind the annual report released Tuesday by the Canadian Security Intelligence Service. In it, the agency stresses that the key threats to Canadian national security remain extremist terrorism and radicalization by groups like ISIS, as well as the ever-more complex threat of hacking and cyber-espionage. "Ongoing conflicts in

several regions of Africa, the Middle East, Asia, Eastern Europe and elsewhere show no signs of abating and continue to have serious national and international security implications," said CSIS director **Michel Coulombe** in the report. "Since the bulk of such threats originate from (or have a nexus to) regions beyond Canada's borders, CSIS needs to be prepared and equipped to investigate the threat anywhere."

WikiLeaks CIA data breach could expose Canada's vulnerabilities: ex-analyst

Canadian Press, Mike Blanchfield and Jim Bronskill, 2017 03 08

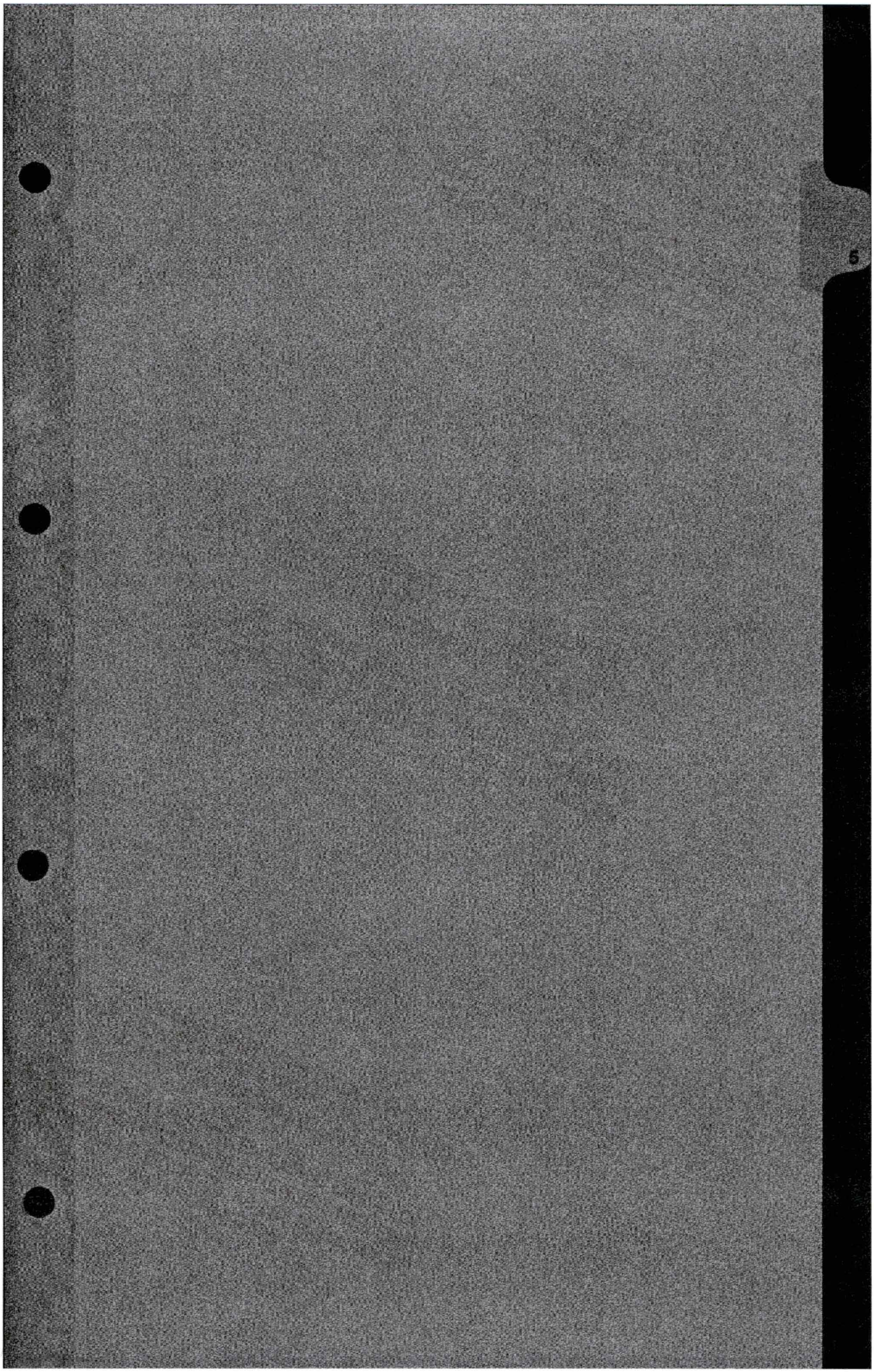
Ottawa - The federal government should be concerned about the WikiLeaks publication of secret CIA files that describe its ability to break into computers, mobile phones and smart TVs, says a former national security analyst. Stephanie Carvin of the Norman Paterson School of International Affairs at Carleton University says Canadian material risks being exposed, since Canada and the U.S. are members of the five-country group of intelligence-sharing countries known as the "Five Eyes." Vulnerable Canadian secrets could include details on the tools and methods Canadian intelligence agencies use to conduct digital snooping. "Because of the sharing between the Five Eyes, if Canada is using some of those tools, yes, our capabilities would be hurt as well," Carvin said in an interview Tuesday. "Secondly, if for some reason, they've been able to get access to some of our documents through Five Eyes sharing, then even some of our methods could be released as well. But we don't know what they have." There was scant mention of Canada in the WikiLeaks files disclosed Tuesday, but one file suggests intelligence agencies took part in a summer 2015 workshop in Ottawa dubbed "Triclops." A memo associated with the event notes an apparent effort to remotely control an iPhone without the user knowing. A spokesman for Foreign Affairs Minister Chrystia Freeland directed questions to Public Safety Minister Ralph Goodale, whose spokesman declined to comment, saying the government doesn't discuss leaked reports. Carvin noted the timing of the leak is clearly favourable to President Donald Trump, given his frequent clashes with U.S. intelligence services. "Anything that kind of discredits the CIA right now is going to be very valuable for Trump," she said. Just last week, the Canadian Security Intelligence Service warned in a public report that the federal government sees serious attempts to penetrate its networks on a daily basis. The spy service tries to analyze networks and malware to uncover clues that help identify the origins of cyberattacks.

Trump torture embrace increases pressure on Canada to repeal directives

Canadian Press, Jim Bronskill, 2017 01 31

Ottawa - U.S. President Donald Trump's embrace of torture is prompting renewed calls for Canada to scrap federal directives that allow the use of information obtained through brutal means. Several human rights groups and the federal NDP are calling on Public Safety Minister Ralph Goodale to repeal the instructions, introduced by the former Conservative government. Goodale has said the ministerial directives raise troubling issues. Since becoming president, Trump has expressed openness to the return of torture during interrogations. Groups including Amnesty International Canada, the Canadian Civil Liberties Association, the National Council of Canadian Muslims and the Ottawa-based International Civil Liberties Monitoring Group said Monday in a letter to Goodale there's a real risk that intelligence-sharing between Canada and the U.S. may again become tainted by concerns about torture. In the House of Commons, NDP public safety critic Matthew Dube asked whether the Liberal government would repeal the federal instructions in light of Trump's "frightening normalization of torture." Goodale said torture is contrary to the Canadian Charter of Rights and Freedoms, the Criminal Code and international conventions to which Canada is a party. A 2010 federal framework document says when there is a

"substantial risk" that sending information to _ or soliciting information from _ a foreign agency would result in torture, the matter should be referred to the responsible deputy minister or agency head. The directive specific to the Canadian Security Intelligence Service, based on the framework, says the agency must not knowingly rely upon information derived from torture. But it adds that in "exceptional circumstances" CSIS may need to share the most complete information in its possession, including details likely extracted through torture, to deal with a threat to life or property.


6

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Protecting Canadians and their Rights: A New Road Map for Canada's National Security
Report of the Standing Committee on Public Safety and National Security (SECU)

Summary

SECU's report provides an overview of the testimony brought forth to Committee during its study of the National Security Framework and Bill C-22, between June 14, 2016 and February 15, 2017. The Committee makes 41 recommendations and requests a Government response to the report, which is required with 120 days of the tabling of the report (May 2, 2017).

As the recommendations are largely based on recurring comments from witnesses, this summary focuses on synthesizing and identifying those recommendations relevant to CSIS. Where appropriate, comments from the report's overview of the testimony are identified underneath their relevant recommendation.

Overall, the Committee concluded that, measures taken to address counter-terrorism threats and ensure the safety and security of individuals should respect the constitutionally protected rights and freedoms of Canadians. This is the primary theme throughout the recommendations.

The Conservative Party of Canada submitted a dissenting report, stating the need to maintain national security tools put in place with Bill C-51. The dissenting report further stated that intelligence to evidence and cyber security issues should have been examined more fully in the Committee's report.

The NDP submitted a supplementary report. While agreeing with the Committee report in principle, the NDP added its own recommendations, including: repeal SCISA and SATA; replace current ministerial directive to prohibit sharing information where mistreatment is possible; enable Committee of Parliamentarians to have full access to information without exempting ministers from the obligation to disclose information.

Recommendations

CSIS specific recommendations – on limiting the use of threat reduction measures and deconflicting with law enforcement:

- #11 – Repeal section 12.1(3) of the CSIS Act to remove the ability to "violate the Charter" with a warrant.
    - **Of note:** The report states there is no definition of "disruption activity" in Canada (p. 20)
    - **Of note:** The report states that some witnesses suggested clarifying what CSIS can and cannot do in using disruption powers in the *CSIS Act* (p.21)
- #12 – Require CSIS to exhaust all other non-disruptive means of reducing threats before engaging in disruptive powers
- #13 - Ensure section 12.1 requires a warrant for all disruption activities violating Canadian law. Ensure Minister's approval must be obtained prior to activity under section 21.1
- #14 - Amend CSIS Act to include a quarterly report on disruption activities for the Committee of Parliamentarians
- #15 – Ensure CSIS de-conflict with the RCMP and other police forces to avoid duplication between police investigations and disruptive powers

Of interest - on restricting the use of preventive detentions:

- #16 – Restrict preventive detention to exceptional, narrowly defined, circumstances and ensure conditions comply with Canadian and international standards on due process
    - ***Of note: The report states that it is *still unclear whether CSIS can detain an individual* (p. 20).

Potential CSIS Impact - on increasing the coordination of review bodies:

- #6 – Consider mechanisms of review / transparency in addition to the Committee of Parliamentarians
- # 8 - Establish statutory gateways among all national public safety and national security review bodies to provide for the appropriate exchange of information
    - **Of note:** The report references that statutory gateways were proposed in the Arar Inquiry and these would go beyond provisions allowing the current sharing of information (p.14)
- # 9 - Increase the funding of all public safety and national security review bodies
- # 10 - Establish a national security review office to serve as the integrated review body for governmental bodies with a national security mandate. The office would serve a coordination role between these bodies; provide a centralized intake mechanism for complaints; report on accountability issues; and conduct public information programs

Of interest – on new review bodies:

- #7 - Create an independent and external review body for CBSA

Potential CSIS Impact – on reviewing Ministerial Direction regarding mistreatment:

- #28 That the Minister of Public Safety and Emergency Preparedness will review ministerial directives concerning torture to ensure that they are consistent with international law

Potential CSIS Impact – on the surveillance of communications:

- #39 – That no changes be made to the lawful access regime for subscriber information and encrypted information.
- #40 – That CSE, in acting upon the requests of other national security agencies regarding the surveillance of private communications and the gathering and retention of metadata, work only with appropriate warrants from the agencies making such requests
- #41 - Adopt a whole of government approach to cyber security strategies (i.e. GCHQ approach)

Potential CSIS Impact – on Intelligence to Evidence and the use of Special Advocates:

- **Of note:** The report states that the Air India Commission recommendation to amend the CSIS Act and require CSIS to share intelligence with the police has never been implemented (p. 31)
- #29 - Amend sections 38 to 38.16 of the Canada Evidence Act to repeal the two-court system for criminal cases and enable trial judges to review secret information and decide on matters of confidentiality.
    - **Of note:** The reports states that having the Federal Court settle applications for disclosure, while trial judges determine the substantive issue of guilt or innocent without access to the undisclosed confidential information, causes unnecessary delays /duplicates efforts (p. 30-31)
- #30 – Amend the Canada Evidence Act to allow the court to appoint special advocates to protect the interests of the accused and of the public in disclosure proceedings. Allow these advocates, with the appropriate security clearance to access confidential government information.
- #31 – Amend sections 83(1) and 85.4(1) of IRPA to give special advocates full access to complete security certificate files.

Of interest – on limiting the scope of SCISA:

- #22-23 – Narrow and redefine the scope of activities subject to SCISA, particularly "activities that undermines the security of Canada"
    - **Of note:** Some witnesses recommended adopting the CSIS' section 2 definition of "threats to the security of Canada" in SCISA. (p. 26-27)
- #24 - Ensure that protections guaranteed under the Privacy Act are not abrogated by SCISA
- #26 – Amend SCISA to adopt a model of dual thresholds: relevance for disclosing institutions and necessity and proportionality for recipient institutions

Of interest – on the review of SCISA:

- #27 – Create an office of the national security compliance commissioner to review all national security information sharing activity between and among government departments/ agencies
- #25 – That the Committee of Parliamentarians conduct an immediate review of the operational evaluation of the information exchange process included in SCISA

Of interest – on preventing /providing efficient recourse for false positives under the Passenger Protect Program (PPP):

- #32-#38 – The report has several recommendations to amend SATA to provide greater recourse to individuals denied air travel, particularly false positive matches, including the nomination of a special advocate.

SUBJECT/SUJET:

Liberal members of the House of Commons Standing Committee on Public Safety and National Security hold a news conference to discuss the report Protecting Canadians and Their Rights: A New Road Map for Canada's National Security.

DATE/DATE:
May 2, 2017 11:30 a.m. ET

LOCATION/ENDROIT:

NPT, OTTAWA, ON

PRINCIPAL(S)/PRINCIPAUX:

Rob Oliphant, Chair, House of Commons Standing Committee on Public Safety and National Security;
Michel Picard, Member, House of Commons Standing Committee on Public Safety and National Security;
Nicola Di Iorio, Member, House of Commons Standing Committee on Public Safety and National Security;
Pam Damoff, Member, House of Commons Standing Committee on Public Safety and National Security;
Sven Spengemann, House of Commons Standing Committee on Public Safety and National Security

TRANSCRIPT:

Moderator: Hello. Bonjour. Good morning. Welcome to the National Press Theatre. I'm Kristy Kirkup from Canadian Press and I will be chairing this press conference.

Today, we're going to be hearing from Liberal members of the House of Commons Standing Committee on Public Safety and National Security. To start off, we'll be hearing from MP Rob Oliphant as well as from his colleague, Michel Picard. I'll let you guys begin.

Rob Oliphant: Thank you. Merci beaucoup et bienvenue tout le monde.

I want to thank you for joining us today. This morning, I had the honour to table in the House of Commons a report of the Standing Committee on Public Safety and National Security, which is entitled Protecting Canadians and Their Rights: A New Road Map to Canada's National Security. The report includes 41 recommendations, primarily in response to the anti-terrorism laws established by the former Bill C-51, but also in response to evidence and testimony that the committee heard during its study.

This study included the kind of broad coast to coast public consultations and expert witness testimony and solid respectful deliberation among Members of Parliament that we believe should have taken place in the last Parliament but did not when the former Conservative government enacted their Bill C-51.

This report clearly notes that there need be no trade-off between national security and the rights of Canadians. They both may be fully realized and in fact, can only be fully realized if they are both fully respected. Among the 41 recommendations, there are some key ones I want to draw our attention to today and that one of the first things we do is we require all warrants for the Canadian Security Intelligence Service, CSIS, to respect the Canadian Charter of Rights and Freedoms.

We'll be requi-, we are recommending the clarifying of overly vague definitions in the Criminal Code, such as terrorist propaganda to ensure that Canadians are not limited from doing lawful protest. Making changes to the passenger protect program, or what is often called the no-fly list, making the program more responsive to complaints and more transparent for all Canadians to understand.

Developing a strategy based on, based in communities for the prevention of radicalization to violence, a national strategy but with local engagement, local priorities. And finally, clarifying definitions of the SCISA, the Security of Canada Information Sharing Act, to ensure that Canadians' privacy is always protected.

I want to mention with thanks committee members on both sides of the House, particularly my colleagues who are with me this morning for collegial thoughtful activity, but also for those in the opposition who engaged well in this process. It's obvious that the Conservative members of the committee did not agree with our report and have issued a dissenting opinion. However, we stand firm that there need be no trade-off between liberty and security. Rather, they are bound together, and we as Canadians value that and that is what we heard from Canadians from coast to coast.

The NDP have offered a supplementary opinion saying that they agree with our report, however would go further, which I think indicates that we have struck an important Canadian balance in the middle between those two extremes and are offering Canadians a chance to have the best security possible, as well as ensuring that their rights are protected.

M. Picard.

Michel Picard: Merci. Ce matin, le président du Comité permanent sur la Sécurité publique et la sécurité nationale a déposé en chambre un neuvième rapport intitulé Protéger les Canadiens et leurs droits: une nouvelle feuille de route pour la sécurité nationale du Canada.

L'étude qui a précédé le dépôt de ce rapport a été motivée par un engagement à revoir les dispositions de la loi anti-terroriste, mieux connue sous le numéro C-51. Le comité a tiré profit de nombreux témoignages d'experts, d'académiciens et de citoyens d'un océan à l'autre. Au surplus, les débats entre parlementaires auront aussi contribué à mieux circonscrire les recommandations que nous portons à l'attention du gouvernement. À trait indicatif, le rapport propose que tous les mandats du Service canadien de renseignements en sécurité respectent la charte canadienne des droits et libertés.

Qu'il faille clarifier un certain nombre de définitions apparaissant dans la loi sur les communications d'information ayant trait à la sécurité du Canada, de même que dans le Code criminel, par exemple, celle de la propagande terroriste afin d'éviter que les Canadiens ne soient restreints inutilement dans leur désir de manifester légalement. Que le programme de protection des passagers soit plus transparent, plus compréhensif, notamment en manière de gestion des plaintes, et que le développement d'une stratégie de prévention de la radicalisation menant à la violence tienne compte de la réalité des différentes communautés.

En fait, s'il y avait un seul message à retenir de l'ensemble des travaux du comité, c'est la primauté de la charte, l'importance, le caractère incontournable qu'il faille absolument garder l'assurance de la protection des droits en même temps que celle de la liberté de tous les Canadiens.

Merci.

Moderator: Okay, and we will now proceed with questions. So to start off, Hélène Buzzetti, Le Devoir.

Question: Mr. Oliphant, I've read most of the recommendations in the report, but some of them go quite far. I was wondering if you have any indication by your Liberal government that they're open to embrace those recommendations. Have you had any discussions?

Rob Oliphant: The government saw this report when you saw it. So what I would say is that the, the report and its recommendations are rooted firmly in platform commitments that were made during the election. The Minister obviously came to our committee and outlined the changes that he was making. We encouraged him. And I think that any recommendations that are beyond the platform requirements that we would see as part of what we wanted to do come out of what Canadians have asked for us to do.

And, and they push into areas like the, the no-fly list, Passenger Protect Program, or some information sharing and also some oversight that I think adds some depth to what the party has already said. And I think this is our role as MPs. Our role as MPs is to not be stuck in the party platform, use it as our base and then drive beyond it to reflect what Canadians have been asking us.

Question: So is it a case of, you know, going further in the hope of getting really what you want? Are you going further than what you think the government is prepared to accept or do you think that this will be entirely –?

Rob Oliphant: I think I would speak for all, all our members here today in saying that this isn't a bargaining position. What this is is a thoughtful and we believe Canadian and Liberal approach to the issues of security and freedom, and making sure that privacy rights are protected and to correct the imbalance that came out of Bill C-51, and to do that in a way that Canadians can have the best laws possible.

It's complex, it's 41 recommendations. It touches on many acts, it's a thorough study. We believe it's a study that should have been done in the last Parliament, but it's not a bargaining position. It is very much a thoughtful exercise. It's been done in parallel with the Minister's own public consultations and we haven't had a report yet on that public consultation. I suspect there will be differences, but I suspect there will be more similarities.

Moderator: Tonda MacCharles, Toronto Star.

Question: Hi. Can you clarify – so I've read this section on disruption warrants and the Liberal platform, you know, said what it seems to me to be much the same thing as you're saying, make sure that the warrants for this kind of activity comply with the Charter of Rights, but can you clarify exactly what you want to happen because many of the experts who examined that section and that power say that it's completely upended. It's backwards anyway, because a judge should not be authorizing a violation.

Rob Oliphant: Correct.

Question: So I don't understand what you want to see. How do you think that that power can be made tolerable?

Rob Oliphant: The first we would say, we heard this in, not unanimously, from testimony but overwhelmingly in testimony, was that the McDonald Commission, which actually was used to set

up CSIS, made a clear distinction between enforcement and intelligence. Those functions used to be blended and over the years, and the Minister said this at committee as well, those have become blurred, those distinctions. And our first call is to, the government, to step back from that and clarify that the RCMP and other police forces in Canada are enforcers and we have a very important security function being done in the intelligence realm, and those two should not be blurred.

We recognize however that at times, our, CSIS has information that they need to act on in a time sensitive way. What we have said about that, first is they will never act, or should never act, in violation of the Charter. That is our primary goal, there should be no exceptions to that, especially by intelligence or police forces, not, you know, that's our bottom line.

In --

Question: So, so I'm, just so I can understand that, so you're saying that in fact, there shouldn't be judicial warrants allowed for disruptive measures that would violate Charter rights --

Rob Oliphant: Absolutely.

Question: -- such, such as, if I could just finish my thought there, so anything like even crashing a website, disrupting someone's travel plans via, you know, their checking in or whatever, that all of that would violate either mobility rights or, or expressive rights. So you're saying that there actually shouldn't be those warrants. That power shouldn't exist in CSIS' hands?

Rob Oliphant: That's right, except Charter rights are always subject to judicial understanding of what Charter rights do have, do embody. What we have said is there are times when things may be against the law, such as break and entry, as some, you know, if anybody in the intelligence area or the police force want to do break and entry, then we're saying two things are required. You need to have a warrant and by judge prior to the activity and also ministerial approval.

So that, that's what we're saying, that there, there are times, we want to make sure that our police and our security forces have all the tools they need, absolutely, so they have that ability, but not to the point of Charter rights being infringed. I'm just going to turn to my colleague, Nicola, and see if you would like to add to that.

Nicola Di Iorio: Power to disrupt is an important power. It has been recognized by witnesses that appeared before the committee. And I'll give you an example: somebody's about to launch a cyber attack that will be extremely detrimental to this country. You obviously want your security forces to be able to disrupt that activity. If they have to turn off the power, for example. You said something crucial in your question, though, because you said that, you were referring to another example, you said that obviously infringes on the Charter.

What we're advocating is that yes, there are situations that clearly violate the Charter, but what we're saying is that there are situations that are in the grey zone and therefore, you need to be in front of a judge who will assess whether it is a violation of the Charter or not. And if it is not a violation of the Charter, the judge will most likely allow the activity to go on. If the judge comes to the conclusion that it is a violation of the Charter, he puts an end to it. There's no further discussion.

Question: But there would not be judicial authorization for intelligence forces to violate the Charter, even if it means for example, crashing a website. This is the power they have now, right? So you're saying take that power away from them?

Nicola Di Iorio: Well, your question's important because you say even for example, crashing a site. Well, a judge would decide whether crashing a site violates the Charter. That's what we're saying. Instead of deciding ahead of time that everything is permissible regardless, we say we live in a country that is governed by the Charter. This is the principle that we advocate around the world, and this is what we want to serve as an example to the world.

So what we're saying is let's go in front of a judge who's trained to interpret and evaluate, knows how to assess the facts and then we'll determine whether it is permissible or not.

Moderator: Charelle Evelyn, The Wire Report.
Question: I wanted to ask about is recommendation 39, it says you know, it doesn't recommend any changes to the lawful access regime in terms of (inaudible) require subscriber data or, you know, accessing someone's mobile device. This is something that, you know, the Association of Police Chiefs has been asking for, saying it'll make their jobs easier. Why is it that you decided that this is not the way to go?

Pam Damoff: Thank you for that, and you're correct. We did hear from the police chiefs advocating for further powers, but we also heard from witnesses who referenced the Spencer Decision and said that they already have the power to do that. They just have to get a warrant. And so we're saying that it's important that they do get that warrant and we're not, we're not recommending that they, the power be expanded.

Rob Oliphant: I might just add to that that overwhelmingly, we recognize that we need to do a 21st century study on cyber security, that these are, you know, we have three recommendations around that area, however, that was not broadly the scope of this study. We heard testimony, we made some recommendations, but more work needs to be done in that area because it's, it is maybe perhaps one of the more constantly evolving issues that we need to take time on.

Question: If I could follow up, from my, maybe I understood it incorrectly, my understanding is that they were asking for, to be able to compel people to give, say, their passwords, for devices seized under a warrant. So you're saying even if, so they, as far as I understand, they don't currently have that, so they can get the devices under the warrant but they can't make you open it. So that, so that they don't currently have that power, so why, why wouldn't you want to give them?

Rob Oliphant: We are arguing that right now, they have sufficient power within the current law not to have more, open however to more study. We needed more time on that issue. But at this time, we're recommending no changes to the regime as it stands. The argument was made. It wasn't yet compelling, but we're also open to the fact that we learn every day. And so we do need to study that more further, further.

Moderator: Omar Sachedina, CTV.

Question: Hi. Some of the issues that you've highlighted in the report have, have already been talked about and addressed at length. I'm thinking of, you know, potential examples of overreach having to do with C-51 and beg definitions. Throughout these consultations, is there anything that, that surprised even you that had not been addressed in the public domain before, that you sort of sat back and said that's not something that has been discussed or not even something that we had thought of previously?

Unidentified Male: We thought --

Unidentified Male: I think, if I, if I (inaudible) --

Unidentified Male: Apart the no-fly list, one thing that I learned, I'm going to share with you, no-fly list, we always look at it as a Canadian problem. What we don't realize when we think about no-fly is that we border the United States and our flights have to fly over that country. So if you go from Toronto to Vancouver, you will be flying over US territory. And therefore, the US has a legitimate right, a sovereign right to determine who's going to be flying over its territory.

So sometimes people are denied access to flying, not because they're on the Canadian no-fly list, it's cause they're on the American no-fly list. That's something that I discovered. I always believed that if they were denied on Canadian soil, it was because it was a Canadian no-fly list. I discovered that it could be because of the US no-fly list.

Michel Picard: Since it goes beyond what was the Liberal Party engagement and the platform, we went much further than just initial engagement and focus on (inaudible) went far. The only idea of reconsidering what is the real threat, the level of threat, so we can assess that correctly brought us to make sure that we asked the right question and get the right level and make proper recommendation, not based on what is already recommended by CSIS, other organization and they, they, it's not surprises as making sure that we were going to the limit of what we can ask and get to the, what can be covered in order to make sure that we go as far as we could.

So it's not rather surprises then make sure that the report brings to the attention of the government a much wider range of concerns that what it was engaged at the first time, in the first place.

Sven Spengemann: If I can just add, this is an excellent question. I think there's a, there were thought processes out there that were in the public realm, but this exercise really sharpened them and brought them to light. And one of them is the importance of public trust in government as being fundamental to specifically this undertaking to, to improve our security but also to uphold our Charter values. It's really the sense that we have to do both, that there aren't any trade-offs and also that we need to be inclusive of communities across our country.

In fact, Ihsaan Garde, who's the Executive Director of the National Council of Canadian Muslims, said that inclusion is a key component of public safety, the inclusiveness that everybody has to have a stake in these two ambitions, which is to safeguard our Charter values and to deliver the most effective possible security across the country. I think this, this really sharpened that view that we thought was out there, but witness after witness agreed with this proposition.

Pam Damoff: Just to say I think what surprised me was also around the Passenger Protect or no-fly list. I have a young man in my riding who's on, whose name is on that list and I think it's important to distinguish between whether it's the person or the name and it's his name that's on the list, that the previous government, for 10 years, didn't do anything to put in place a system that would – in the States, United States, they have the redress system.

We didn't have anything designed in Canada to allow people to get a redress number like they have in the States. And the fact that that went on for the last 10 years, and that's why we're recommending that we do put in place a redress system so that people like this young man can apply and get a number that does allow him to fly and have his, that individual have a much easier time flying, which is in place in the United States and nothing was done here for 10 years, to put in place a system that they can get redress if their name is on that list.

Rob Oliphant: I might add to my general feeling on this topic was that I believe this is a modest report and it's modest in that we start out very early saying what we don't know. And our response as the majority on the committee is to say when we don't know something, we want to learn more. And so the first couple of recommendations around getting that threat assessment report out there and to do more research and develop more capacity in these broad areas.

Our response is not knee-jerk to close down society because we don't know things. It's not to, to stop citizens' rights and privacy because of lack of knowledge. Instead, we reach out, we reach out to marginalized communities, reach out to those who may be excluded because of racism or sexism or other issues. We reach out to bring people in and study. And that's not a passive kind of activity. It's a real activity to say we don't know enough. We need more expertise, more money for research and more transparency around what the real threats are to Canada. And then through that, we'll be guarding rights, protecting them and making sure we have a safe country.

That, that actually felt good that I thought we, as a country, knew more, and we actually need to know more.

Moderator: (inaudible)

Question: What happens next? I mean, some of the issues, like C-51, it was a flashpoint during, during the campaign. A lot of Canadians, you know, if you bring it down, this report for the average Canadian, you know, who want, who want action on this, they've been waiting for action on some of these things, what do you tell them and who might just fear that this is just another report and now, it'll be up to the government to decide what to do?

Michel Picard: Such an easy question. Thank you. I'll start in French and I'll do it in English, because it's a very, that's the point of the whole thing.

Quarante-et-une recommandations sur un sujet que le gouvernement antérieur avait dit il y a rien à refaire sur ce qu'on a fait dans C-51. L'ancien gouvernement prétend que C-51 est correct, adéquat, parfait, il y a rien à refaire. Les gens ont démontré au-delà des engagements du parti Libéral en campagne, au-delà que quelque attente que ce soit, ont démontré la grande quantité de modifications, des points sur lesquels il fallait apporter une attention particulière pour justement améliorer ce qui vraisemblablement faisait défaut.

Alors, toute prétention à l'effet que le système d'avant était adéquat, nous on ne fait que rapporter ce que les gens ont conclu à l'effet que non, voici ce dont nous avons besoin.

It's an obvious, we have to realize that what has been done in the past is clearly not sufficient based on the fact that we ended up with 41 recommendations. If C-51 was right on, we wouldn't need those, that many recommendations. People have, have said, talked, explained, shared, exchanged their concern because we needed those modifications. We just put that together. As Sven said, we sharpened everyone's opinion to have a clear picture of what is needed for us, then to send it to the government's attention.

So any, anyone who pretends that what was in the past was fine maybe is missing some part of it.

Rob Oliphant: I might add on that that the government has an agenda on this issue. They're working, government moves slowly. We as parliamentarians are out there in our ridings. We're hearing this issue and so we did the study to, to push, to absolutely push on behalf of the people we

represent. So that, that's a purpose of the study. We're, there is no lack of confidence in what the government is doing. What we're saying is more.

So we're strongly supportive of Bill C-22, and the oversight measure of putting in a committee of parliamentarians and we're also then saying that's a great start. We also want independent oversight of CBSA, the Canada Border Services Agency. We also want oversight of the 17 agencies that have some intelligence security aspects to them that don't have oversight. We're looking for that. And we're looking at a legislative gateway that looks at all the agencies and makes sure that they're able to do joint studies together and it's the appropriate amount of, of information sharing. And we're also encouraging government – this is a political part – to say you need to resource, fund, support those agencies commensurate with the expanded activities.

So if you have an RCMP, or a CSIS or a CBSA or a Security, Communications Security Establishment, if you have those bodies that have broader mandates and more people working there, you need to up the oversight and that relates, I think, to what Mr. Spengemann has said about confidence and trust. Oversight and review are good for the agencies. We're just asking for more.

Moderator: (off microphone) we're just going to go Hélène, and who has second round of questioning, so Hélène first and then (inaudible).

Question: Okay, I just want to go back to this oversight thing, because recommendation number 10, I believe, proposed the creation of a overseeing body of oversight, kind of thing, but where you also recommend to have more bridge between the oversight mechanism. So I just want to know is that, is that contra-, not contradictory but is that a duplication? How, why do you need both?

Rob Oliphant: We don't think so. We think that there's one thing that is a statutory gateway which requires and facilitates the conversation appropriately between oversight agencies so they don't duplicate work. So we don't end up having to have an O'Connor or a Iacobucci inquiry or commission. We don't want to do that. We think that it should be integrated into the system so that's a statutory function.

We're also suggesting that there be an office, a national security review office – I would have put it in capital letters – (laughter) that, that is responsible for the appropriate integration of that activity and also those other agencies which don't have as their principal mandate national security but have, Transport Canada has some security function. There's many parts of government, there are 17 bodies that have some aspect. You're not going to set up a whole body for them, but you set up an office that, that monitors them.

And, and we got into the difference between review and oversight. Most of what we're talking about is review, looking at past activities in that office; in the bigger agencies, we're looking for oversight that is real time.

Question: So as a supplementary, I just wanted to go back to Tonda's questions about the, voyons, perturbations, --

Michel Picard: Disruption?

Question: -- disruption, thank you – the disruption powers, so correct me if I'm wrong, what you're saying is that because now currently, and correct me if I'm wrong, I believe you need a mandate from a judge only if what you're about to do is contrary to the Charter. Right? And now

what you're saying is that you want to go in front of a judge for every case of disruption and if the disruption is contrary to the Charter, it will be refused. Did I get this right?

Michel Picard: Correct. But there is no other way. I mean, if we say that there can no longer be the power to disrupt, if there's a violation of the Charter, it does imply that you have to go in front of a judge every time because otherwise, you'd be judge and party. You would be deciding well, it doesn't violate the Charter, you know, we're just going to be, you know, doing this horrible thing, but we don't feel it's violating the Charter.

What I want to stress is that, you know, the fact that you put in legislation as it was in C-51, that you can violate the Charter, what you're basically doing is you're leaving your citizens at the mercy of individuals who have maybe other priorities on a given day, and you know, what we always have to be mindful and remind the Canadian people is that when you give a power like that, it's not necessarily used against the bad guys. It could be used against the good guys or mistakenly perceived as bad guys.

And then you wind up in a situation where you damage the Canadian brand because people look at this and list what kind of situations we have in those countries and then you have a mega investigation going on as to why this happened and why did we (inaudible) that situation? Well, we can see it with C-51.

Pam Damoff: Could I just add to that? I think it's important to remember that we take security very seriously. But there was an example that was given when we were hearing testimony of surveillance and how people want to make sure that they're protected, but the idea of having a camera in their house that would monitor their home 24/7 where someone was watching just in case there was ever a break-in is not something that people would be comfortable with.

So it was, it struck home with me that example of, of yes, we want to make sure that we're safe, but would I be prepared to have a camera in my home 24/7 monitoring me? No I wouldn't. So I think, you know, that was a very concrete example of where it would be going too far, in my opinion. So I think, you know, we need to be mindful that we do take security very seriously, but we need to be also cognizant of the privacy of individuals.

Unidentified Male: I think just to go back to your question about the range of 41 recommendations, some of them are complex or governance related, some of them are very simple. Like the Security Infrastructure Program, for example. It's an existing program, and we had faith leaders come up to us through this process and in our communities as well, to say we have congregations from, from a range of different communities who are now fearful to exercise their faith in their places of worship.

So this program was up and running, it was being used and the simple reflex for us was to say we should, we should do more. We should fund it more and we should make sure that communities are aware of the parameters of this program, which basically allows them to install perimeter security even inside the places of worship as well, cameras, fencing, and ID checks and those, those kinds of things, right? So some, some recommendations exist. They're part of the basket and we're simply saying we need to ratchet up and to respond to the rather fluid and changing security environment that we're in.

Moderator: Are there any other questions? This conclu-, oh.

Rob Oliphant: I was just going to say thank you for this and to publicly again thank my colleagues for their, their work. This is obviously a passionate issue for many Canadians and it's been borne out in the passionate work of the committee members.

Question: (off microphone) (laughter) minority dissenting report by the NDP --

Rob Oliphant: A supplementary report.

Question: A supplementary report, you're right, you said that you're somewhere between the two extremes, but I was, I was wondering why you use that word since the NDP maybe does not go as far to its extreme than the Conservatives do. So can you just (off microphone)?

Rob Oliphant: I think in their first recommendation in their supplementary opinion, they call for a repeal of all acts affected or touched by C-51, and we don't think that's a responsible way of approaching it. That would be the difference. I mean, they're in agreement and accord with our report except they would then repeal all of it, and we're saying no, the safety and security of Canadians is entrusted to, to parts of those acts and we want to make sure that their rights are also equally recognized in that process, no trade-off.

So we just don't believe that that's a responsible way of governing. We think the responsible way is to actually do the hard work of the 41 recommendations. They're not all easy to get into, but it is, yeah, in some ways it's simpler, you know, to just repeal. That's not what we're about, so we would not go to that extreme.

Michel Picard: La qualité des témoignages que nous avons reçus a démontré une approche relativement raisonnable de l'ensemble des témoins. Rien d'extrême. L'équilibre que Mme Damoff a parlé au niveau de la liberté des droits a été retrouvé dans la plupart des témoignages. Donc, si l'ensemble des Canadiens qui s'expriment pour emmener ce genre de rapport suggèrent une approche raisonnable équilibrée, mais probablement que ceux qui avaient des vues extrêmes, comme notamment le NPD a changé un peu son approche en réalisant que finalement, d'ailleurs quelques-unes de leurs recommandations font aussi partie du lot, finalement l'approche raisonnable plus équilibrée s'avère plus représentative de la volonté des Canadiens.

Rob Oliphant: And lastly and not only because I think they're watching, but to thank our Clerk, Jean-Marie and our analysts and our staff that did hard work. This was a long study and it was a demanding study, so I want to make sure that out there, they know that they are thanked.

Moderator: Thank you very much.

Michel Picard: Oui effectivement, nos pensées vont à toutes ces personnes qui nous ont soutenus tout au cours de cette démarche. C'est un travail très exigeant, très rigoureux qui demande une attention à une foule de détails, et ils étaient toujours présents, toujours disponibles, toujours attentionnées et certainement dévouées et très travaillants. Alors on les remercie pour tous ces beaux efforts.

Moderator: Thank you.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 049 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, December 8, 2016

Chair

Mr. Robert Oliphant

Standing Committee on Public Safety and National Security

Thursday, December 8, 2016

● (1530)

[*English*]

The Chair (Mr. Robert Oliphant (Don Valley West, Lib.)): Good afternoon. I'm very happy to call to order the Standing Committee on Public Safety and National Security's 49th meeting in this Parliament and to welcome our guests.

I want to welcome Mr. Aboultaif and Mr. Vandal as full members of our committee today. We're glad to see you.

Welcome, Minister Goodale, and thank you for accepting our invitation to help the committee pursuant to our Standing Order 108 (2) study of the subject matter of supplementary estimates (B) for 2016-17.

We'll be considering the supplementary estimates. Just a reminder to the committee that due to scheduling we were not able to consider the supplementary estimates (B) prior to their having been deemed accepted by us and already reported to Parliament. However, not ever wanting to miss an opportunity to spend time with the minister, we are very pleased that he's able to be with us.

The topic of the first hour is the supplementary estimates (B) and other issues related to those, which I'm sure will arise.

In our second hour of the meeting, we'll continue with Mr. Coulombe from CSIS to discuss recent events and the Noël decision in the Federal Court.

Obviously, members, you know you can ask questions of anybody, but I'm thinking that if we could hold most of the questions for Mr. Coulombe until the second hour, it would probably be somewhat more efficient, but the time is yours.

I just want to draw your attention to the working document, the issues and options paper on Canada's national security framework which was sent to committee members this afternoon. Check your inbox and take a look at the issues and options paper. I have not had a chance to look at it yet, but I know in advance that it will be good work, so I thank the analysts for their work.

Mr. Goodale, the floor is yours.

Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness): Mr. Chairman and members of the committee, thank you for the invitation to be here today particularly on supplementary estimates (B).

I'm very pleased to be joined by most of the usual cast of characters: my deputy minister Malcolm Brown; Michel Coulombe, the director of CSIS; Commissioner Paulson from the RCMP; and Caroline Xavier, who is vice-president of operations at the Canada Border Services Agency.

I would point out that the former president, Linda Lizotte-Macpherson, has retired as of last Friday, and her replacement, John Ossowski, is in the process of arriving. He will no doubt have the pleasure of appearing before the committee on future occasions. In the meantime, Caroline is representing CBSA today.

Fraser Macaulay, assistant commissioner with Corrections Canada is also here, as is Harvey Cenaiko, the chairperson of the Parole Board of Canada.

As you will note from studying the supplementary estimates (B), the department portfolio of Public Safety is requesting adjustments that result in an increase in our spending authorities of $256.3 million. I would like to run through very briefly what the items are that add up to that total.

Canada is, as you know, a safe and peaceful country, but we also know that we are not immune to threats, including natural disasters, terrorism, and other crimes and acts of violence. The women and men of the public safety portfolio, including the department itself and all of the various agencies that you see represented here today, do the essential and often dangerous work of protecting Canadians, and for so doing they deserve and I believe they have our admiration and our gratitude. It's up to us as parliamentarians to support them and their work so that they can continue keeping Canadians safe and protecting the rights and freedoms that we all hold very dear. The items included in the estimates are directed toward that end.

First of all, let me deal with Fort McMurray. As you know, we faced a terrible fire disaster there earlier this year, probably the worst in Canadian history. In coordinating the federal response to that disaster, I got to see some pretty remarkable things, including the courage of the people of Fort McMurray, the determined leadership of local, provincial, and federal officials, the skill and the selflessness of firefighters, police officers, and other first responders, and the tireless efforts of the Canadian Red Cross, and of course, from coast to coast, Canadians gave generously to support those who were so seriously affected.

The Government of Canada has transferred $104.5 million to the Canadian Red Cross, honouring the Prime Minister's commitment to match the individual charitable donations that were made by Canadians in support of Fort McMurray. That accounts for a large portion of the total authorities that are being requested today, those matching funds for the Red Cross.

Also, under the disaster financial assistance arrangements, we made an advance payment to Alberta of $307 million as a down payment on what will be the ultimate obligation to assist Alberta in dealing with this disaster. That amount of money is not in these estimates because it is covered in the main estimates. Every year there's an allotment for the DFAA, and the amount that's required for Alberta is covered in the allotment in the main estimates. The supps deal with the matching money for the Red Cross of $104.5 million.

The second topic is HUSAR, the heavy urban search and rescue teams. That capacity in Canada is something we mentioned in our election platform saying that we would reinstate federal funding to support the HUSAR teams across Canada. They are absolutely indispensable in responding to such emergencies as ice storms, floods, wildfires, building collapses, and so forth.

The previous government made a decision at one point to eliminate this funding. We decided it was of sufficient priority that it needed to be reinstated. In October I was pleased to deliver on the commitment we had made by launching the heavy urban search and rescue program, which will provide $3.1 million annually in funding for these heavy urban search and rescue task forces. This program will not only support and strengthen the four existing task forces in Vancouver, Calgary, Brandon, and Toronto, but they will also help to develop new capabilities in Montreal and re-establish capabilities in Halifax. To this end, $3.1 million is being sought through supplementary estimates (B).

● (1535)

The third major topic is RCMP class actions. Another part of the mandate that I received from the Prime Minister was to take action to ensure that all parts of the public safety portfolio are healthy workplaces, free from all forms of harassment. I've been working on this from the very beginning of our mandate, notably inviting the Civilian Review and Complaints Commission for the RCMP to undertake a comprehensive review of RCMP policies and procedures on harassment, and also appointing Sheila Fraser as a special adviser to examine the RCMP's complaints process and the treatment of complainants. That work is ongoing. I expect to hear from both of those processes sometime next spring.

I was also very pleased to join Commissioner Paulson on October 6 for the announcement of a $100-million settlement between the RCMP and a large number of plaintiffs in two proposed harassment-related class action lawsuits, of which $40 million is being sought through these 2016-17 supplementary estimates (B). The remaining $60 million will be accessed in the following year. In addition to the $40 million for actual payments for settlement, there is another $17 million for class action counsel and claims assessment being sought through these estimates. The total amount required to deal with the class actions is $40 million plus $17 million, for a total of $57 million.

I think we should be encouraged by this development and by the eloquent apology that was offered by the commissioner. We continue to advance other initiatives on this very important front of safe workplaces. This is an important step in helping us move forward from a deeply troubling aspect of the history of our national police force to a much different future.

In terms of the claims process, I think it's important to highlight that, totally separate and apart from government, totally separate and apart from the force, an independent process has been set up to actually adjudicate the claims. The RCMP will have no involvement except to make documentation available. The government will have no involvement except to provide the funding. The decisions will be made by the Honourable Michel Bastarache, a former justice of the Supreme Court of Canada, who is the independent assessor. He will make the determinations of the appropriate amounts, case by case by case.

On national security, the government continues its work to ensure that Canada's national security framework keeps Canadians safe while safeguarding our rights and freedoms. I'm pleased to report that the unprecedented engagement with Canadians that we have launched right across this country has been very successful, including a series of town hall meetings, round tables, public hearings, personal discussions, and meetings with subject matter experts, as well as quite literally tens of thousands of contributions coming in via email in our online consultations. That consultation remains open until December 15, but already the total number of participants is in excess of 45,000 Canadians. It's a very encouraging number.

Once again, let me thank the committee for the hearings that you held and the report you will make about the advice you would offer the government in relation to the national security framework. We are analyzing all of the input, and we will be putting forward a set of measures that will be designed to achieve two objectives simultaneously: protecting the public, keeping them safe and secure, and at the same time safeguarding the rights and freedoms of Canadians in a free, inclusive, and democratic society.

I also want to note the work the committee has done on Bill C-22. I understand it's now in the process of being reported back to the House, and I will be very anxious to consider that report.

● (1540)

One other matter under national security which involves an estimate in these supplementary estimates (B) is the creation of the office for community outreach and counter-radicalization to violence. That item was earmarked in the budget last spring, and to this end, you will note in these estimates that my department is seeking $2.3 million in 2016-17 to establish and staff the office as well as support the domestic programming and research initiatives through a newly established grants and contributions program called the community resilience fund.

The office will provide leadership on Canada's response to radicalization to violence, coordinate domestic and international initiatives, support programming and research, and enhance our expertise. We simply must become very good at this initiative if we want to retain that fundamental character of Canada as an open, inclusive, democratic society.

Immigration detention is another item I want to mention today. We are requesting $22.7 million this fiscal year to support the Canada Border Services Agency in its implementation of our new national immigration detention framework. A total of $138 million for this initiative was announced in August, spread over a number of years. In this first year we're asking for $22.7 million.

The goals of the new framework include: first, expanding practical, workable alternatives to detention; second, significantly improving conditions at immigration holding centres, including better mental and medical health services; third, reducing our reliance on provincial facilities; and fourth, reducing the number of minors in detention to the greatest extent possible.

Of the funding that's being requested for this year, $21.3 million is being directed to the construction of new immigration holding centres in Laval, Quebec, and in Surrey, British Columbia. These facilities will help reduce the reliance on provincial correctional facilities for immigration detention.

The balance of the funding this year will be used to begin enhancing medical services within our immigration holding centres and to implementing alternatives to detention so that, as much as possible, immigration detention remains a measure of last resort and not first resort.

A great deal is under way. A good many things have been achieved, but there is, of course, always much more to be done. My officials and I are happy to try to respond to your questions today. We look forward to working with the committee on a whole array of national security issues for the future.

Thank you.

● (1545)

The Chair: Thank you, Minister.

For the first round of questioning, we'll begin with Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): It's nice to see you, Minister Goodale. It's good to have you and your team back in front of the committee.

I would like to ask you to give us a bit more of a fine-grain view of your vision for the immigration detention facilities and the changes thereto. Is this analysis one that's driven by numbers? Is it driven by qualitative differences or challenges you have alluded to in terms of youth being detained? How do you see this framework evolve over, let's say, the next five years?

Hon. Ralph Goodale: There are only three federal immigration holding centres in Canada: in Surrey, British Columbia, right at the airport in Richmond, in Laval, Quebec, and in Toronto. Those are the largest intake centres for newcomers arriving in Canada, so logically the federal facilities would be there.

They are often overtaxed in terms of volume. The next resort is to rely upon provincial correctional facilities in the neighbourhood to deal with people where detention is the only alternative.

The numbers, we feel, in these various federal and provincial facilities are simply too high, and we believe the provincial facilities, in particular, are problematic because they are correctional facilities. The people who are being detained for immigration purposes are intermingled—

Mr. Sven Spengemann: There's a stigma issue, if I can interrupt.

Hon. Ralph Goodale: There is, and we want to get rid of that as much as possible.

The reason for detention is really only in three particular cases. One is when there is a real problem in identifying who the person is. Identification is obviously a critical factor in assessing safety considerations. Often CBSA is not able, with the information available to them, to precisely identify the individual. If there's an identification issue, if there is a flight risk, or if there is a serious risk to the public, then detention becomes an alternative that CBSA can consider as a last resort. The problem with the circumstances of the past and up to now is that there aren't very many other resorts to consider, so detention too often becomes the default mechanism.

We want to improve the three facilities to make sure they can handle more people in a better way and take the reliance off the provincial correctional facilities. Also, we want to make sure that in those federal holding centres the appropriate mental health and physical health services are available, that legal counselling and other counselling is available, and that inspections can be done by the Red Cross and by the UN High Commissioner for Refugees, as and when necessary, at their discretion. We also want to make sure that there are other physical alternatives to detention. We're discussing with a whole variety of immigrant support organizations what those alternatives might be.

The Toronto bail program, for example, has been used as a good example of what an alternative might look like. There may be electronic means, voice identification, or new technology that could be of assistance. CBSA officers will have a broader array of alternatives to look at to keep the public safe and to make sure that the people who are in the circumstances of detention are dealt with in a proper and humane way. When it comes to children, as much as possible we want to eliminate that altogether.

Mr. Sven Spengemann: Thank you very much for that.

Minister, in the transfers under public safety, there's a $41-million transfer from PSEP to the Royal Canadian Mounted Police for first nations community policing. This committee had the former correctional investigator of Canada, Mr. Howard Sapers, here recently to comment on the 2016 report. Could you let the committee know your vision of what needs to happen in first nations policing?

The argument we often hear is that our correctional facilities are overcrowded because of the upstream challenges that may exist. Could you give us an update as to what your thoughts are in the context of this $41-million transfer?

● (1550)

Hon. Ralph Goodale: Both the justice minister and I have mandate instructions from the Prime Minister to work with all dimensions of the criminal justice system to deal with the very negative consequences of that system for a great many indigenous people. Minister Wilson-Raybould, as you know, has a whole range of laws and procedures under consideration.

One of the dimensions of it that relates to my portfolio is the first nations policing program. That program was established in the early 1990s. The last minister to actually give it a policy facelift was solicitor general Herb Gray in 1996. It hasn't been improved in terms of policy since that time. I give Mr. Gray a lot of credit for what he did back then, but that's over 20 years ago, and it's time to bring the policy up to date. It also has not had a financial increment since 2009.

It is basically a 50/50 arrangement, or almost 50/50—it's 52/48—between the federal government and the provinces. We each contribute an amount to the first nations policing program and then try our best to provide, in consultation with first nations communities, good solid policing services, but with the amount of money that's available and the policy framework that's available today, we're not nearly meeting the need. Probably not much more than half of the communities that could quality for this kind of service actually have it.

The objective here is to bring the policy up to date so that indigenous communities can count on top-notch policing services that are equal in terms of standards and professionalism to the policing services that every other group of Canadians takes for granted, to make sure the cultural sensitivity is there in the way the service is delivered, and to make sure there is adequate financing on a long-term basis.

Many of the first nations have said to us that we should really think of whether or not a first nations policing "program", which implies that it's temporary, is the right way to go when we're providing a fundamental service such as a police service, and maybe there should be a more comprehensive and permanent basis for the way in which all governments come together to ensure safety in first nations communities.

Mr. Sven Spengemann: Thank you.

The Chair: Thank you, Minister.

Mr. Clement.

Hon. Tony Clement (Parry Sound—Muskoka, CPC): Thank you, Minister, for being here.

I wanted to start by allowing us to elaborate a bit on our exchange in the House of Commons today and talk about that Canada Border Services Agency report on the Mexican drug cartels, and the concern expressed in the CBSA report that removing the visa requirement in fact extends the reach of the violent drug cartels to expand into Canada. In particular, there was a concern that they merely would replace the fentanyl shipments from China that we're trying to crack down on with more cartel shipments from Mexico.

I want to give you the opportunity to respond for a bit more than 35 seconds on that. It was not a concern that I was aware of before this report was made available to a journalist—an internal report of the CBSA—but now it's of grave concern. We do not want to see increases in fentanyl and increased deaths because of fentanyl or any other harmful drugs in our society. We don't want to see the increase in violence that normally attends with the Mexican drug cartel.

On the one hand, you have lifted the visa requirement, and on the other hand, we have this concern expressed by Canada Border Services Agency officials. I want to give you the floor to answer more fully than we could do in Parliament.

● (1555)

Hon. Ralph Goodale: Mr. Clement, whenever a decision is taken with respect to border arrangements, the decision is taken with a great deal of care and deliberation to make sure that all the proper analysis has been done and that we are accomplishing two objectives. One is a properly functioning, efficient, successful border, and the other is that all of the factors in relation to public safety and security are properly dealt with.

In dealing with inflows of people from every part of the world, CBSA takes their function at the border very, very seriously. Whether or not a person arrives on Canada's shores with or without a visa, they are obviously examined at the border to determine if they can enter Canada. Coming to Canada without a visa isn't a free pass to get in. The CBSA officers do their job at the border to identify if there is any risk or danger: is there a need for secondary clearing; is the person admissible or inadmissible in all of the factors that CBSA takes into account? All of this has been weighed very, very carefully to ensure that we have the police, the security, and the CBSA resources and authorities lined up to keep Canada's borders safe and secure.

We obviously are very concerned, as are our colleagues in the provinces and our colleagues in law enforcement, about this phenomenon that has swept across the country in the last number of months related to opioids.

Hon. Tony Clement: Yes, sorry to cut you off, but I have limited time, Minister.

I just want to read directly from the CBSA report, which says, "The visa lift will make travel to Canada easier in order to establish or strengthen existing cartel smuggling chains. In the next three years, Mexican drug cartels are expected to expand their presence in Canada by sending operatives and recruiting local airport or marine port workers with ties to Mexico."

This is not a case of the natural flow of trade. This particular section of the report looks specifically at the visa lift and said that we are creating additional problems for ourselves involving the Mexican drug cartel.

Your point is well taken that CBSA does what it can, but clearly they are raising red flags for all of us. It is our responsibility to respond to those red flags, so how are you responding to those red flags?

Hon. Ralph Goodale: First of all, there has been a long series of discussions with the Mexicans to ensure that we have the appropriate system in place, both in Mexico and in Canada, to keep Canadians safe and secure, and that the visa lift can be done in a way that is successful for both countries.

On the Canadian end of the equation, through the good work of CBSA and law enforcement by the RCMP and others, we are putting in place, as we always do, systems that will protect Canada. CBSA has done its job in flagging an issue that they want themselves and the rest of government to pay careful attention to, and we are, to make sure that this can be done in a successful way.

Hon. Tony Clement: Could I ask you, Minister, to undertake to this committee and to Parliament to continue to report to us on the efficacy of these ways and means under your disposal and under CBSA's disposal to ensure that they are working to curtail the influence of the drug cartels? In the alternative, can I ask you to have an undertaking with us that if, for whatever reason, those are not working to your satisfaction, you would initiate a review of the visa lift in order to protect the safety of Canadians?

● (1600)

Hon. Ralph Goodale: Mr. Clement, it's a fundamental responsibility of government to monitor its programs and its activities. That is especially true in the field of public safety and security. We will be examining very carefully all of the activities we undertake to make sure we're accomplishing the objective that this department has the responsibility for.

I'm happy to share our progress reports with the committee. I suspect that from time to time the committee may ask the question, but even without being asked the question, we'll be happy to keep you posted on the progress we're making.

In relation to opioids in particular, and not related to any particular situation, let me make three or four points.

Hon. Tony Clement: If you could make one or two.... I don't know how much time I have left.

The Chair: We're running into a bit of overtime—

Hon. Ralph Goodale: Okay. Maybe we'll come back to opioids.

The Chair: —but you can have another half a minute. Go ahead.

Hon. Ralph Goodale: We're looking at the border measures that are required to be effective at the border. CBSA and the RCMP have already interdicted a number of shipments, which already shows a pretty impressive capacity to exercise those kinds of controls. We're looking at what else needs to be done to strengthen the situation at the border. As you know, we're already engaged in a diplomatic initiative, with the Chinese in particular, to get international co-operation to stop this scourge at the source.

[*Translation*]

The Chair: Thank you.

We will continue with Mr. Dubé.

You have eight minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

Minister, thank you for being here with us.

I'd like to talk to you about Judge Noël's ruling concerning the retention of data by CSIS.

The day after the decision, when you spoke to the media, you were asked whether it was appropriate to retain data on persons who do not constitute a threat to national security. You answered that that question had to be looked at and that you were willing to hear the opinion of both camps to decide how to follow up on that.

Something worries me about those words, and perhaps you could give me some further details on this. I hope you are not opening the door to this type of practice, that is to say the retention of data on persons who are not a threat to national security.

[*English*]

Hon. Ralph Goodale: We are examining all of the facts of the matter, Mr. Dubé, to determine what the appropriate policy should be going forward. As you will know, Mr. Justice Noël himself commented on the fact that the legislation might be needing an update since it was written at a time when the fax machine would have been considered groundbreaking technology. Things have changed since then.

He raised the question of whether or not the legislation itself needed an upgrade and a modernization. We will consider all of the factors that are relevant in these circumstances. Indeed, the national security consultation that we launched some months ago is examining a variety of these questions—

Mr. Matthew Dubé: Minister, if I may, I'll interrupt, because my time is limited and it's the only crack at this that I'll get.

You're not closing the door, then, to the possibility of this happening again. To me, it seems that if the Federal Court has deemed this to be illegal, then the answer should be clear. If you do want to update the legislation, wouldn't an appropriate proposal be to make sure that CSIS has the statutory obligation not to retain data on people who are not considered threats to national security?

Hon. Ralph Goodale: I'm receiving advice from a lot of Canadians about all of these issues. When we put that all together in the national security framework, we will report to Canadians on what the result is, but bear in mind that there are two objectives for this consultation: number one, keep Canadians safe; number two, and equally important, simultaneously safeguard the rights and freedoms of Canadians in an open, inclusive, and democratic society, and that includes their privacy rights.

We have had some very important advice offered just in the last number of days from Commissioner Therrien, the federal Privacy Commissioner, and a number of his provincial counterparts. I take the advice coming from the Privacy Commissioner very, very seriously.

● (1605)

[*Translation*]

Mr. Matthew Dubé: To the extent that retaining data is a breach of the right to privacy, if we want to both ensure security and protect rights, it seems to me that it is easy to say that we will not retain data on persons who are not a threat to national security, since there will be no consequences for national security. I will leave that for the moment, but this is certainly not the last time I talk about it.

I would like to put my question to your colleague the Minister of Justice, but since you are here, I will put it to you.

Some Department of Justice lawyers went to court to defend what CSIS had done. Were you or your colleague the Minister of Justice aware of the arguments put forward by the Department of Justice?

[*English*]

Hon. Ralph Goodale: Which defence are you referring to, Mr. Dubé?

Mr. Matthew Dubé: I'm referring to the Department of Justice lawyers' going into court, omitting certain information, and defending this scheme by CSIS. Were you or the Minister of Justice aware of this?

Hon. Ralph Goodale: In addressing this question, the director of CSIS and the deputy minister of justice have both said clearly and unequivocally that until the Federal Court made its ruling, they were of the view, based upon their own legal advice, that the procedures being followed by CSIS were, in fact, authorized by the statute.

Mr. Matthew Dubé: So you were not aware?

Hon. Ralph Goodale: No. The first time this issue came to my attention was in the SIRC report for 2014-15, which was filed in Parliament in January of this year. It should have been filed last year, but it was delayed because of the election.

Mr. Matthew Dubé: There were several months between January and the court ruling and then the media coverage that followed. What happened in the meantime? You were aware in January, and then the decision came out later. Did you have a discussion with CSIS? How did this play out?

Hon. Ralph Goodale: The SIRC report flagged the issue. It was after the issue had been raised by SIRC that the Federal Court began its further examination of the issues that were involved. The service and the Department of Justice were dealing in an ongoing way with the Federal Court, responding to its questions and providing it with information. That was an ongoing process over a period of several months.

Mr. Matthew Dubé: Was data retention still ongoing, or was there a moratorium while these court proceedings took place? What exactly happened? I'm still unclear on that.

Hon. Ralph Goodale: When the issue was fully elaborated on by the court, Mr. Justice Noël provided us with a copy of his judgment. When I had the opportunity to read his judgment, I immediately called upon SIRC, since it was the body that had raised the issue in the first place, to reinject itself in the situation to make sure that the judgment of the court was fully and properly enforced. Mr. Coulombe advised me that that, in fact, was the case.

[*Translation*]

Mr. Matthew Dubé: Do you not find it worrisome that when you arrived in your position as Minister of Public Safety and Emergency Preparedness, you were not made aware of this activity by an agency that is under your supervision, and were not informed before a few months had gone by, at least before January, according to what you said?

[*English*]

Hon. Ralph Goodale: The agency, the service, and the deputy minister of justice were dealing with an outstanding legal issue. They informed me that they were responding to the questions of the court. They were providing information. They were collaborating with the court in every way to provide the information that was required. This was an ongoing procedure.

When the court finally issued its opinion on the subject, which was in about the middle of October, I believe, that's the point in time when I had the opportunity to read the court's judgment. The court said, as you have reported, that it found this particular retention of associated data to be without legal authorization in the statute. It's at that point the director of CSIS took the immediate step to stop the practice. I invited SIRC to re-involve itself in the situation to supervise and to make sure that the data was properly taken care of in accordance with the judgment of the court.

● (1610)

[*Translation*]

Mr. Matthew Dubé: Perfect.

In the wake of the comments by your colleague the Minister of Natural Resources, can you assure us that aboriginal activists are not under supervision at this time, with regard to the demonstrations that will certainly be held after the announcement about the Kinder Morgan Trans Mountain project? We learned that this had taken place in the past. Can you assure us that this is not a practice that is used currently, for prevention?

[*English*]

Hon. Ralph Goodale: I can give you the absolute assurance, which we made reference to in our election campaign, that peaceful protest, demonstrations, and advocacy are fundamental rights in Canada. They're protected by the charter, and if necessary, we will change the law to reinforce those rights, to make it absolutely clear that Canadians can exercise those democratic rights without fear in this country.

Mr. Matthew Dubé: We'll follow up on that.

Thanks, Minister.

The Chair: Mr. Mendicino, you are next.

[*Translation*]

Mr. Marco Mendicino (Eglinton—Lawrence, Lib.): Thank you, Mr. Chair.

[*English*]

Minister, thank you very much for your remarks this afternoon on the supplementary estimates, and for taking a moment to expand on a number of priorities that relate to your portfolio. It's quite clear to me, as I would think it would be to all members of this committee, that there is a tremendous amount of work that is being done on the portfolio, and for that we are very grateful.

You made a recent announcement with regard to the security infrastructure program. For those who are unaware, this is a program that is designed to help communities that are at risk of hate-motivated crimes to improve their security infrastructure.

Could you take a moment to tell us how you've enhanced the criteria and the eligibility of this program in ways that improve on the old model?

Hon. Ralph Goodale: Thank you, Mr. Mendicino.

This is not an expensive program. It costs about $1 million a year, so it's not a program that involves a huge amount of public funds, but it is a very useful program for groups and organizations that feel themselves to be vulnerable to hate crimes. Sadly, we have seen in recent weeks and months some very painful examples of that.

We've had some pretty brutal graffiti, vulgar in nature and quite crude in its dissemination of white supremacist symbols, in my own city of Regina. Here in Ottawa, four places of worship were subjected to this kind of attack. We've seen it in Toronto. We've seen it in Peterborough, and in other places across the country.

Groups and organizations that feel themselves to be vulnerable have, over the last number of weeks and months, made the point that the security infrastructure program, while useful, could be made more useful without costing a lot more money by changing the terms and conditions of the program, so we have broadened the eligibility requirements.

One of the previous rules was that you had to have suffered an attack in the past in order to qualify for the funding. The funding is available for gates, fences, security film on windows, closed-circuit television, cameras, lights, those sorts of things that contribute to public security. As I said, in order to be eligible for it in the past, you had to have had an attack which is kind of like prevention after the fact.

We've changed that. Obviously, if you have had an attack, you're still eligible. Now, however, if you can demonstrate your vulnerability in advance by objective evidence that shows you may be vulnerable to this kind of danger, you can submit that argument to the Department of Public Safety and Emergency Preparedness, and the officials will make an assessment. You can actually, as a part of your application, get an external opinion about the vulnerability. That's one important change.

Another change is to make the security infrastructure expenses applicable to the inside of a building, and not just the outside of a building. Previously, it was just the outside perimeter. Now it can include infrastructure changes within the building.

Another thing we're doing is making sure that communities that may feel vulnerable are well informed about the program. We're involved in a communications effort to reach out to groups and organizations, to let them know that the program is available and that they're eligible to apply if they think it would be appropriate and necessary.

● (1615)

Mr. Marco Mendicino: I will certainly do my level best to help educate the members of my community on this program. This is an issue that has come up in my riding of Eglinton—Lawrence as well, so we are grateful for these enhancements.

In my remaining few minutes, I would like to ask you to expand for a few moments on the Fort McMurray fire that you characterize as being one of the worst natural fire disasters in the history of the country. You mentioned that we have matched, in these supplemental estimates, the $154.5 million in contributions made to the Canadian Red Cross, and before that there was $307 million set aside in the annual disaster relief fund.

Can you tell us how those funds will be used to help the community in Fort McMurray recover from this terrible disaster?

Hon. Ralph Goodale: The two separate programs, the matching funds and the DFAA, are designed in a way not to overlap with each other or conflict with each other. The funding through the Red Cross is aimed at those sorts of things that DFAA would not cover.

There are three sources of assistance here. One is the official disaster financial assistance arrangement where, according to a preset formula depending on the magnitude of the loss, a portion of the loss is paid for by the Province of Alberta, and a portion of the loss is paid for by the Government of Canada. The bigger the loss, the larger percentage the federal government pays.

So far, federal and provincial officials have identified $307 million that the Government of Canada will need to contribute to the Province of Alberta. That is not the final calculation; that is an advance payment. So far, it's $307 million. As the work goes on to rebuild the community and the losses are identified in more precise terms, losses that aren't otherwise covered by insurance, the tally will no doubt continue. It does take usually some years for these things to be totally tallied up, but we were able to put into the hands of the Province of Alberta, within one month of the fire, $307 million to begin the process of supporting Alberta in dealing with the situation.

The Red Cross money is aimed at things that would not be covered under the DFAA. The Red Cross has done an amazing job. The total funds that were donated, which they were able to collect from generous Canadians across the country, was $185 million. The federal matching was $104 million, and there was matching on top of that by the Province of Alberta for another $30 million. The total in the Red Cross fund is $319 million to assist those impacted by the fires, including $227 million to support individuals and families, $50 million to support community groups that are involved in the rebuilding and the rehabilitation, and $30 million to support eligible small businesses.

● (1620)

The Chair: Thank you, Minister.

Mr. Miller.

Mr. Larry Miller (Bruce—Grey—Owen Sound, CPC): Minister, it's always great to have you here.

Lady and gentlemen, thank you to all of you for being here.

Last week, Minister, we had the corrections investigator at committee. We questioned him about the review that was being undertaken. One of the recommendations was to increase inmates' pay. I think there would be many Canadians who would be dismayed that any kind of allowance or pay would go to prisoners. He seemed to be under the impression that this increase is necessary, and he's quite content that inmates never use their pay "to purchase illegal drugs".

Do you agree with that?

Hon. Ralph Goodale: I think Mr. Sapers is very well positioned to examine the facts. His advice is that that very small amount of funding is not, in fact, used for any illicit processes.

Mr. Larry Miller: Is there documentation, a study, that shows that, and if so, could the committee get a copy of that?

Hon. Ralph Goodale: Perhaps I could ask Fraser Macaulay to comment on that from the point of view of the Correctional Service.

Fraser, if you could, also just describe the amount of money that's involved, which is relatively small. Again, remember this was a recommendation from Mr. Sapers.

Mr. Larry Miller: Understood.

Hon. Ralph Goodale: I have simply passed that recommendation to the CSC and invited them, as Mr. Sapers had asked, for the issue to be investigated.

Mr. Larry Miller: I appreciate that.

Hon. Ralph Goodale: It's under investigation. It's not a decision that has already been taken.

Mr. Larry Miller: Okay, thank you.

My next question was going to be for you anyway, Mr. Macaulay, so continue with that.

Chief Superintendent Fraser Macaulay (Assistant Commissioner, Correctional Operations and Programs, Correctional Service of Canada): We would have to take an undertaking to see where he has determined those facts. I can assure you that we don't have a breakdown of the complete spending of their funding to that level—

Mr. Larry Miller: Okay.

C/Supt Fraser Macaulay: —but we would be able to do that.

Mr. Larry Miller: Sure, I appreciate that.

My next question is also for you. We hear all the time, and even Mr. Sapers was around it, that there is a drug problem within prisons, some of it is illicit drugs, some of it—and for the life of me I can't figure out how or why—is prescribed drugs. There's a problem there, so how do we fix this? I don't think it's a perceived problem. I think it is a problem, with the amount that you hear about it.

Do you have any comments?

C/Supt Fraser Macaulay: There is no doubt that there are several inmates who come in both with substance abuse issues and/or casual drug usage, and that during their time in incarceration, whether it's using medications and/or other illicit means to get drugs in, that is done. It's an ongoing issue for us.

We follow very strict plans, from our searching inside, to education, to actual health interventions, to programming interventions. We're following the same as any outside public domain would, attacking the issue from three components.

Yes, there is no doubt that drugs do get in. There is an active market for people who are seeking that relief both inside and outside of institutions, and it is an issue that we attempt to deal with as much as we can.

Mr. Larry Miller: Okay.

On the drugs getting in, Mr. Macaulay, in this day and age of technology and security, and what have you, you'd think you could pretty well stop it if the will was there. Even if they were coming in, let's say, by drones, I would think that before the prisoners are let out for their daily exercise, security would check the yard to make sure nothing had been dropped in.

It's pretty hard for a layman or the average person to figure out why we aren't stopping it if we really want to. I'm not pointing fingers, but it would appear to me that it should be able to be stopped.

● (1625)

C/Supt Fraser Macaulay: I don't disagree from a perspective of talking to the average person and their beliefs of the prison system and incarceration levels and the security levels that we have.

Unfortunately, where there's a will, there always appears to be a way. There are illicit drugs that get into our institutions, whether it's through personal importation or from people going in and out of the institution that we're missing during our searches. As an example, the new synthetic drugs are very hard to stay atop of, even from a technical perspective. The more we change our formulary to pick it up, quickly the same issues get picked up and different types of substances are being done. So—

The Chair: Thank you, Mr. Macaulay.

C/Supt Fraser Macaulay: It happens, but it's not obviously what we want to happen.

Mr. Larry Miller: Time always goes way too fast.

Thank you.

The Chair: When you're having fun.

Thank you, Mr. Macaulay and Mr. Miller.

[*Translation*]

Mr. Di Iorio, you have five minutes.

Mr. Nicola Di Iorio (Saint-Léonard—Saint-Michel, Lib.): Thank you, Mr. Chair.

Minister, thank you for the time you devoted to the preparation and presentation of your statement. I also thank your collaborators.

I'd like to speak to you about borders and customs. There is a problem I would like to bring to your attention involving reception, appearance and wait times.

I will begin with the reception issue. People who come to our borders, to customs, are either Canadian citizens, that is to say people to whom this country belongs, or people who are not Canadian citizens. It seems to me that there is a these people should be received with a minimum of civility.

Which brings me to the second problem, that of appearance. When we arrive at Canada border posts, we see that our agents are dressed in quasi-military garb and that the organization seems almost military. The one-size-fits-all approach seems to be a problem. It is one thing to arrive at the Montreal airport, but it's another to arrive at a border post in a rural area.

The third problem involves wait times. It seems unacceptable to me that we make a Canadian citizen who is coming back to his own country wait.

I brought this problem to your attention in a general way by deconstructing it, Mr. Minister. I would like you to tell us about the measures that will be taken by our government to solve this situation.

[*English*]

Hon. Ralph Goodale: Mr. Di Iorio, the Canada Border Services Agency has an incredibly difficult and important job to do. They are charged with the responsibility of maintaining security at Canada's borders. That's a serious business. The safety of the country depends on them making the proper judgments at the border about what comes in and who comes in, and what doesn't come in and who doesn't come in. That's a really profound assignment.

At the same time, they are making decisions at the border that have a huge impact, good or bad, on the Canadian economy. Just think of the border between Canada and the United States. There are 400,000 people who cross that border every day, and there is about $2.4 billion in trade that crosses that border every day.

CBSA is a fundamentally important organization. They have to get it right. There's a real seriousness about this job.

At the same time, you make a valid point that when Canadians are returning home, or when newcomers are arriving, they want to feel that they're being treated professionally, politely, and in a welcoming fashion.

● (1630)

[*Translation*]

Mr. Nicola Di Iorio: Mr. Minister, when I go to China, I am received better there than in my own country. The country is a dictatorship; there have been no elections like ours for a long time. However, the people there are not dressed like the military, although it is a dictatorship supported by a military regime. In my country, I cannot get the same reception.

That is why I used the expression "one size fits all". We seem to be using the highest level of security needed for certain situations. These officers see 400,000 people go by day after day, but they cannot establish criteria to determine whom they should spend less time with and whom they should spend more time with.

[*English*]

Hon. Ralph Goodale: Well, it's a careful balance, Mr. Di Iorio, and Canadians would be pretty unforgiving if they found that the system in some way didn't serve them well on the security point of view. At the same time, there needs to be that human element that also is welcoming and polite.

Maybe I could ask Caroline Xavier to comment on this, because these are the kinds of questions that she has to deal with every day.

[*Translation*]

Ms. Caroline Xavier (Vice-President, Operations Branch, Canada Border Services Agency): Thank you, Mr. Minister.

We invest an enormous amount to train our officers and we make sure they conduct themselves in a very professional manner. Customer service is very important for us. Mr. Di Iorio, I understand the comparison you are making between China and ourselves. I can tell you that we look at what is being done internationally to find ways to improve our border services on a daily basis.

We are very proud of the way in which we serve the public. There are certainly things that we must continue to improve and we still have a lot to learn. By analyzing other organizations around the world that are responsible for border services, we will gain an understanding of how to improve those services, and that includes the feedback you gave us today.

We also receive a lot of positive comments about the services we provide to Canadians and to other travellers who cross our borders daily.

I understand what you are saying about security. However, as the minister said a few minutes ago, we are the first point of contact for the public and we take that very seriously. We want to make sure that the people arriving here are those who should be coming into the country.

I fully understood your comments that sometimes the officers see the same person on a daily basis. For cases like that there are programs, such as the NEXUS program, that allow those who cross the border frequently to enter the country more easily.

The Chair: Thank you, Ms. Xavier and Mr. Di Iorio.

It is now time to—

[*English*]

Mr. Larry Miller: On a point of order, I just wanted to verify that we could get that information I requested, Mr. Chair.

The Chair: Okay. We'll make a note of that in the minutes. Thank you.

[*Translation*]

My thanks to all the witnesses for joining us today.

[*English*]

Thank you for your time and for your testimony. We'll take a brief pause as we change to go to the second hour.

● (1630)

(Pause)

● (1635)

The Chair: We're going to continue now with the second part of our meeting.

It was the committee's request to spend a little more time with officials from CSIS. We're very pleased that the director, Mr. Coulombe, is here with us, as well as Mr. Cousineau, who is here as the assistant director. We also welcome, from the Department of Justice, Mr. Frater, chief general counsel.

I understand that the director has a statement. Members should have copies of it.

We'll give them time to make a statement, and then we'll proceed to questioning.

Welcome.

[*Translation*]

Mr. Michel Coulombe (Director, Canadian Security Intelligence Service): Thank you very much, Mr. Chair.

Thank you for giving us the opportunity to talk about a very important issue today.

As Canada's national intelligence service, the mandate of the Canadian Security Intelligence Service, CSIS, is to identify, investigate and advise government of threats to the security of Canada.

To fulfill our mandate, we rely on a range of investigative techniques. Irrespective of the technique employed, operational activity must be authorized, reasonable and proportionate; this, in consideration of the nature of the threat.

[*English*]

When required, and with the approval of the minister, CSIS may make an application to the Federal Court to obtain warrants against subjects of investigation. These warrants, which are granted by the Federal Court, authorize the use of specific investigative techniques in accordance with specific conditions identified by the court as appropriate.

One such technique is the interception of communications. When CSIS intercepts communications, it obtains the content, as well as the associated data linked to that communication. Associated data is the context, not the content, of a communication. Such data is used by computer systems to identify, describe, manage, or route communications across a network. On its own, it does not identify individuals who are party to a communication.

Whereas CSIS analyzes the content of communications intercepted under warrant to determine whether or not it is to be retained or destroyed, and continues to do so, in 2006 CSIS adopted the position of retaining and exploiting associated data to enhance our ability to detect threats. It is important to know that CSIS collects this associated data legally, through warrants issued by the Federal Court. At issue, however, is the service's retention of associated data lawfully collected under warrant and, in particular, our decision to retain all such associated data, including that which may be non-threat-related associated data linked to third party communications.

● (1640)

[*Translation*]

The Federal Court also clearly pronounced on the service's duty of candour, finding that CSIS had breached its duty of candour by not informing the court of its position on the retention of associated data and the creation of the Operational Data Analysis Centre, commonly known as ODAC. I can assure you that this was not deliberate.

I agree that the court should have been informed earlier of our approach to the retention of associated data and the establishment of the program. Key government stakeholders were informed of these matters. Former ministers of public safety, the Office of the Privacy Commissioner, the Security Intelligence Review Committee and the Inspector General of CSIS were all briefed on the existence of ODAC and the value of data analytics to CSIS investigations. Clearly, the service was not attempting to keep our data analytics program a secret.

[*English*]

Mr. Chair, as I stated in my remarks on November 3, I accept the court's decision, and I have taken immediate action to respond. I acknowledge the court's serious concerns, and I am committed to continuing efforts to address them.

Immediately after the court decision was issued, CSIS halted access to and analysis of all associated data. While we did so out of an abundance of caution, the service has begun to allow access to and use of the associated data of threat-related communications. We did so because the service unquestionably has the authority to retain this information, and its use is necessary to protect public safety. Efforts are also under way to develop and implement appropriate policies and procedures that clearly address the court's concern. I would like to note that the decision acknowledged the value of data analytics to the service's investigations.

CSIS and the Department of Justice are also working together closely to develop measures aimed at ensuring that we meet our obligations to the court in matters of transparency and duty of candour. I would also note that, as indicated by the Minister of Public Safety, SIRC has been briefed and will be reviewing the service's response to this decision and submitting a report to the minister.

[*Translation*]

Mr. Chair, and members of the committee, let me be clear: CSIS, in consultation with the Department of Justice, interpreted the Canadian Security Intelligence Service Act to allow for the retention of non-threat-related associated data linked to third party communications collected under warrant.

Though it is now clear that the Federal Court disagreed with this interpretation, and we accept this, CSIS was not knowingly exceeding the scope of the Canadian Security Intelligence Service Act.

I wish to reiterate that CSIS recognizes the importance of compliance with the Canadian Security Intelligence Service Act, as well as openness and transparency with the Federal Court.

And with that, Mr. Chair, I will conclude my remarks and welcome any questions.

The Chair: Thank you, Mr. Coulombe.

We will start with Mr. Di Iorio.

You have seven minutes.

Mr. Nicola Di Iorio: Thank you, Mr. Chair.

Thank you, Mr. Coulombe. My thanks to your colleagues as well for taking the time to prepare and present their remarks.

Mr. Coulombe, first, let's go to page 3 of your presentation. The first question that comes to my mind is: has the act changed?

● (1645)

Mr. Michel Coulombe: Are you asking me if it has changed since the decision?

Mr. Nicola Di Iorio: You wrote that the act allowed the retention of the data. As I read the paragraph, I get the impression that you are implying that the act has changed.

Mr. Michel Coulombe: No. the paragraph reads: "...CSIS, in consultation with the Department of Justice, interpreted the CSIS Act...."

Mr. Nicola Di Iorio: So the service came up with an interpretation that was approved by the Department of Justice at the time. Is that correct?

Mr. Michel Coulombe: The service's interpretation of the act was based on advice from the Department of Justice.

Mr. Nicola Di Iorio: So that advice went back to 2005 at least, if not even earlier.

Mr. Michel Coulombe: Yes.

Mr. Nicola Di Iorio: My understanding is that that interpretation, which had been supported by Department of Justice officials, was rejected by the Federal Court.

Mr. Michel Coulombe: That is correct.

Mr. Nicola Di Iorio: Do any aspects of that ruling give you the right to appeal?

Mr. Michel Coulombe: We had the right to appeal, but the decision was not to do so, and to accept the ruling of the Federal Court.

Mr. Nicola Di Iorio: I am not asking this question to annoy you or to distance myself from the decision in any way at all, but so I can really understand.

Do you not think it would have been useful to have a clarification from the Supreme Court of Canada on a matter like this? If the nine justices of the Supreme Court had clarified the matter, Canadians would have had a more complete picture of the situation. Is there anything that would explain the reluctance to ask for that clarification?

Mr. Michel Coulombe: Because that is a legal question, I am going to turn to Mr. Frater, if I may.

Mr. Nicola Di Iorio: Yes, please feel free.

Mr. Robert Frater (Chief General Counsel, Department of Justice): I prefer to answer in English.

[*English*]

There are many reasons to appeal or to not appeal, and this is a very long judgment that deals with a lot of subjects. A large number of the subjects dealt with were dealt with to our satisfaction. It was primarily about setting terms and conditions for warrants going forward. We were quite satisfied with that part of the decision.

With regard to the part of the decision dealing with the duty of candour, we acknowledged to the court that we had breached our duty.

Ultimately, I think what the court was saying was that there should, perhaps, be more clarity in the legislation, rather than seeking clarity.... We always have a choice about seeking clarity: should it be done through legislation or litigation? Our choice here, I think, is in some measure about what should be the subject of legislation and what should be the subject of further clarity through litigation.

[*Translation*]

Mr. Nicola Di Iorio: Thank you, Mr. Frater.

Mr. Coulombe, let me go over the sequence of events again. Your service asks for advice about whether a project you are planning is in compliance with the act. As you have to collect and retain information, you want to know whether you are collecting and retaining it appropriately. I am summarizing, but the answers you received authorized what you were doing.

For how long did people act on the basis of that advice?

Mr. Michel Coulombe: The analysis program was started in 2006 and Justice Noël's decision was rendered in 2016. So it happened over a period of 10 years.

Mr. Nicola Di Iorio: It happened over a period of 10 years.

As I understand it, when the decision was rendered, your service changed its approach out of caution, correct?

Mr. Michel Coulombe: Yes, that's right. As I mentioned, the decision deals with a section of the associated data we collect and retain. When Justice Noël rendered his decision, we stopped accessing and analyzing all the associated data, in order to analyze the decision more thoroughly and to put mechanisms in place that would allow us to resume the program with the data we can retain.

Mr. Nicola Di Iorio: So, there were legal opinions.

At the bottom of page 2 of your presentation, you indicate that, at the time, the Minister of Public Safety, the Office of the Privacy Commissioner, the security intelligence review committee and the inspector general were all aware of it.

● (1650)

Mr. Michel Coulombe: They had been made aware that the program was in place, yes.

Mr. Nicola Di Iorio: Okay.

Did the judge deal with the reasons why the Privacy Commissioner did not react to that information?

Mr. Michel Coulombe: No. Actually, Justice Noël said that he did not express an opinion on the entire matter of privacy in his decision.

Mr. Nicola Di Iorio: My question was actually more specific. The judge paid no attention to it?

Mr. Michel Coulombe: No.

Mr. Nicola Di Iorio: You were criticized for your lack of transparency and candour. However, you told the Privacy Commissioner what you were doing.

Mr. Michel Coulombe: Once again, Mr. Frater can comment on that. However, the Federal Court decision deals with our responsibility to be transparent and candid with the Federal Court. Despite the fact that we had advised the departments, SIRC and the inspector general, we had failed in our duty and responsibility to be transparent with the Federal Court.

The major reason why I included that in my comments is to show that the intention of the service was not to keep this program secret. We were not trying to hide the existence of the program. We advised people, except the Federal Court, and that was a mistake.

Mr. Nicola Di Iorio: How many opportunities did you have to reveal what you were doing to the Federal Court?

Mr. Michel Coulombe: An opportunity certainly arose when the program was created.

As indicated in Justice Noël's decision, the program's existence was mentioned at one point in 2011, but only in passing. According to the Federal Court, it was not done thoroughly enough to really allow the program itself to be understood, especially the fact that we were retaining all the associated data.

The Chair: Thank you, Mr. Coulombe and Mr. Di Iorio.

We now move to Mr. Clement.

[*English*]

Hon. Tony Clement: I just want to make sure I understand exactly what is going on now.

Mr. Coulombe, you still retain the information but have closed access to it. Is that right?

Mr. Michel Coulombe: Yes, in terms of the information that is subject to the ruling, it is still retained, but no one has access, and no one can use it in terms of doing analytics.

Hon. Tony Clement: Then you say efforts are also under way to develop and implement appropriate policies and procedures that clearly address the court's concern. Are you working on a policy that would then regain access to the information consistent with the court judgment? Is that what you are working on? Why are you keeping the information if you do not have access to it?

Mr. Michel Coulombe: It may be important to note that Judge Noël did not order the destruction of the information in question. At the moment, we're keeping it because we are continuing our analysis of the decision and what it means for the impact on the organization.

There could also be other reasons why we do not want to destroy the information at this time.

Rob, is there anything you want to add?

Mr. Robert Frater: No.

Hon. Tony Clement: I'm sorry, are you saying something?

Mr. Robert Frater: There's nothing to add.

Hon. Tony Clement: Yes, I'm sure.

I'm just trying to figure something out. Let me just be theoretical here. Is that information theoretically hackable?

Mr. Michel Coulombe: No.

Hon. Tony Clement: Why would you say that?

Mr. Michel Coulombe: It is because our system is not connected to the outside.

Hon. Tony Clement: Okay. What if you have someone from the inside who has access?

Mr. Michel Coulombe: There is always the insider threat, yes, but again, there are a number of measures the service is taking, not just with that specific data bank, but with all of our holdings in terms of mitigating the risk of insider threat.

Hon. Tony Clement: So the risk is mitigated, but it is not impossible.

Mr. Michel Coulombe: Like any risk, you cannot say you'll bring it down to zero.

Hon. Tony Clement: So, as citizens, we basically have to be trusting in your ability to be perfect in order for this information not to be somehow misused by nefarious forces in the future.

Mr. Michel Coulombe: As I mentioned, there is a risk. You cannot bring that risk to zero.

● (1655)

Hon. Tony Clement: I do want to register, Chair, my disquiet about the data still being in the system when the commissioner made it clear he understands that the court decision means he doesn't have access to that information.

Mr. Michel Coulombe: I can give you one example of why we're doing further analysis. Let us say some of that information that is subject to that decision was used in any type of proceeding in the context of a criminal case or an administrative case, and we destroy that information. Then, if we go back to Charkaoui II, the Supreme Court decision told the service that when you're using information in a court context—criminal, administrative, tribunal—you have to retain that information. Before we rush and destroy that information, we have to make sure that, by destroying it, we're not going to be contravening another court decision, in this case the Supreme Court decision known as Charkaoui II.

Hon. Tony Clement: That's a perfectly reasonable example. What percentage of the associated data relates to that situation?

Mr. Michel Coulombe: That's what we're trying to do now. It is extremely complex to go back—and I can ask John to explain why—into that data bank of associated data and to do that analysis of what is threat related and non-threat related, what was used before, what was not, and what could be safely destroyed.

We have to take the time to do that analysis before we start destroying that information, if that's the decision.

Hon. Tony Clement: You're going through the analysis to decide if a subset of the data can be safely destroyed, but you haven't made the decision to safely destroy the data.

Who makes that decision? Is it the minister?

Mr. Michel Coulombe: No, it would be me, obviously informing the minister as things progress. It would be informing the minister, and as the minister mentioned, he has asked SIRC to review what we're doing as a result of that decision and to report back to the minister.

Hon. Tony Clement: Okay, but it sounds like you haven't made that decision yet—

Mr. Michel Coulombe: No.

Hon. Tony Clement: —so the data is still there.

What does this operational data analysis centre do if you don't have access to the data?

A voice: Do you want to take this question?

Mr. John Cousineau (Assistant Director, Operations Enablement, Canadian Security Intelligence Service): Good afternoon, Mr. Chair. Thank you for the opportunity to appear before the committee today.

As Director Coulombe mentioned, associated data and intercept is but one means of collecting information that the service has. Advanced analytics is used to essentially maximize the value of information that the service collects.

As you can imagine, given that we have other programs that collect information, the advanced data analysis in ODAC is still undertaking analytic work to help move investigations forward, just simply not looking at associated data.

Hon. Tony Clement: So it does other analysis not connected to the associated data, and does not need the access to the associated data to continue its analysis in other matters.

Mr. John Cousineau: Correct.

Hon. Tony Clement: I want to go back—

The Chair: Very briefly.

Hon. Tony Clement: —to your description of the data on page 1 of your remarks, where you say, "Data is used by computer systems to identify, describe, manage or route communications across a network."

Could you be a bit more specific as to what we're talking about exactly?

Mr. John Cousineau: Associated data is data about a communication. It defines not the content of the communication, but it defines the communication event. The purpose of associated data is to help the network route to the information through the network.

A very simple example would be that associated data would be a phone number, so the number that is called. Well, the reason that associated data is there is to actually route the telephone conversation to the right destination. That is what we were trying to explain when we said that associated data is used by the network to actually deliver information.

Again, to reiterate, associated data does not describe the content of the communication. It simply describes the context. Classic examples would be date, time, duration, phone number dialled, etc.

● (1700)

The Chair: That's it.

Monsieur Dubé.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

I am trying to reconcile the Federal Court definition of associated data with the way in which you seem to be defining it. In English, the definition was:

[*English*]

> ...collected through the operation of the warrants from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defense, or international affairs.

[*Translation*]

When you talk about the associated data of threat-related communications, there seems to be a contradiction.

Mr. Michel Coulombe: Actually, you are right. In his decision, Justice Noël himself said that his definition of "associated data" may differ from the service's definition. I must admit that it may be a little confusing. The section of data that Justice Noël decided that we could not retain constitutes his definition of "associated data".

Mr. Matthew Dubé: I go back to Mr. Clement's remarks about the way in which you determine which data you are retaining and which data you can have access to in the circumstances you have described.

If your definition is different from the judge's, how can we be assured that you are not in the process of reusing the data that Justice Noël said it was illegal for you to retain?

Mr. Michel Coulombe: First, we said that we were in the process of amending our policies and procedures. There is an adjustment in terminology, but the terminology matters little. Justice Noël's decision is clear: If the information is not threat-related and linked to third-party communications, we cannot retain it. Whether we use the term "associated data" or some other term, we are complying with the decision, which applies to non-threat-related associated data linked to third-party communications.

However, I quite agree that the terminology and the definitions are confusing.

Mr. Matthew Dubé: You have been reworking your definitions and the terminology since that time. However, how do we deal with the fact that data have been retained under one definition and now, following a judgment that makes the retention illegal, you are changing the definitions, but still keeping that data?

I am having difficulty making sense of all that.

Mr. Michel Coulombe: Maybe John will be able to clarify it.

In the database containing all the associated metadata, some of that data was the subject of Justice Noël's decision. When the decision was rendered, we stopped accessing the database in its entirety. Now we are resuming access to the data that we are clearly able to identify as threat-related. We are able to retain associated data that is threat-related. The judge was clear on that. As we determine the nature of the data, we make them accessible once more so that they can be analyzed.

Mr. Matthew Dubé: How do you determine which associated data are threat-related and which are not?

Mr. Michel Coulombe: I will let John answer that.

But I can say that when associated data is threat-related, an operational report is produced. We are able to establish the link, that is, to go back to the operational report and find the associated data that was used to produce the report. That is how we work.

John, do you want to add anything more specific?

Mr. John Cousineau: I can't really add a great deal. The director is correct, it is just a comparison. We check whether a report has been produced and, if so, we can link it with the associated data. So that is data we are able to retain.

Mr. Michel Coulombe: Perhaps I would like to add that, as part of that analysis, if we cannot clearly determine that the pertinent analysis is linked to a threat for which a report was produced, we err on the side of caution and we leave it in the section that is not accessible.

Mr. Matthew Dubé: Since my time is limited, I will change the subject, although I have other questions about what we are currently discussing.

You mentioned the various people who were made aware of this program. One of them was the former Minister of Public Safety. However, Mr. Goodale does not seem to have been made aware, except through the SIRC report.

Why were former ministers aware, whereas Mr. Goodale was still not aware several months after he took up his duties?

● (1705)

Mr. Michel Coulombe: In 2006, the minister was briefed because we were implementing the program. We advised the minister at the time that we wanted to implement the program, and we told him about its usefulness.

Over the years, the program was mentioned in the annual report that the service must submit to the minister, for example. In the past, ministers have been informed either through the annual report or through the public report produced by the service.

In the case of Minister Goodale, I would have to check, but as for previous ministers, in the annual report that we produce for the minister—

Mr. Matthew Dubé: No briefing is given to a minister coming into office in a new government?

Mr. Michel Coulombe: Yes, there are briefings, but it's important to understand that the program we're talking about is a component of various other programs.

Mr. Matthew Dubé: Thank you.

[*English*]

I think I have about a minute left.

Mr. Frater, I don't know if you can answer this question, but was the current Minister of Justice aware of the arguments that were being made before the court by the Department of Justice about this data retention?

Mr. Robert Frater: She was briefed on the litigation generally. On the specifics of the argument, I don't think so. I don't recall whether she was given a copy of our written submissions, but she was generally aware of the litigation.

Mr. Matthew Dubé: Thank you.

[*Translation*]

Mr. Coulombe, I only have a few seconds left. Obviously, you don't have that information at your fingertips, but you can provide it to the committee. I am curious to know the numerical relationship between the number of people for whom you have the related data and the number of people who were the target of the investigations. I would like to know that proportion.

Mr. Michel Coulombe: We'll try but, once again, because of the nature of the database architecture, it can be extremely difficult to find out how many people were involved.

Mr. Matthew Dubé: Which might speak volumes about the problems of collecting this kind of data, right?

Mr. Michel Coulombe: Not necessarily. It shows that when metadata is put in a database, no link is established between the data and the individuals. We're talking about telephone numbers, emails, IP addresses. It's difficult to determine how many individuals that represents, simply because there is no link.

Mr. Matthew Dubé: Isn't it exactly when we don't know who is connected to the data that we run the risk of making a mistake and involving people who are not a threat?

Mr. Michel Coulombe: That's exactly the meaning of the decision.

The Chair: Thank you, Mr. Coulombe.

[*English*]

Ms. Damoff.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thanks to all of you for being here today.

I'm following up on something that Mr. Dubé started asking you about, and that was previous ministers. I note that this practice started 10 years ago, in 2006, which is the time of the previous government. The previous public safety minister was briefed on the creation of this practice, and I'm assuming that he approved of it.

Mr. Michel Coulombe: Well, I would have to go back.... I don't think that at the time we were seeking his approval. We were informing him that we were putting that program in place.

Ms. Pam Damoff: But he didn't ask you to stop—

Mr. Michel Coulombe: No.

Ms. Pam Damoff: —and then he was briefed on it annually. Is that what you're saying?

Mr. Michel Coulombe: Well, not just that minister, but on a number of occasions.... Just give me a second. For example, from 2007 to 2010, the service actually described the program and what it was doing. Every year, the director has to submit a classified report to the minister. From 2007 to 2010, ODAC, that program, was mentioned in that report. Again in 2010, there was also a verbal briefing given on ODAC and its usefulness to the minister at the time.

Ms. Pam Damoff: Okay. So no one during all those years questioned the privacy of the information and whether you should be doing that, then.

Mr. Michel Coulombe: I cannot comment on whether or not that question was asked at the time. There's no documentation.

● (1710)

Ms. Pam Damoff: Okay. That's fair.

Last December our current public safety minister was sworn in and then found out about it in January, when SIRC released their report. What did the current minister ask you to do when he found out about the SIRC report?

Mr. Michel Coulombe: Well, the SIRC report didn't say, "What you're doing is illegal". The SIRC report only raised the issue that, according to SIRC, the service had not fully briefed the Federal Court on this program.

Ms. Pam Damoff: Okay. Our minister mentioned something today about asking you to take some measures when he found out about it.

Mr. Michel Coulombe: Well, when he found out about the court decision.

Ms. Pam Damoff: Okay.

Mr. Michel Coulombe: When the court decision came out this fall, then the minister.... Actually, we had already taken measures such as stopping access and analysis. That's what the....

Ms. Pam Damoff: Okay.

This is metadata, right?

Mr. Michel Coulombe: Yes.

Ms. Pam Damoff: We've talked about that before.

Mr. Michel Coulombe: Yes, just to make it even more confusing, it's metadata that—

Ms. Pam Damoff: I know. That term kept coming up a lot. I think you described it as nothing more than what's on the outside of an envelope, you and Commissioner Paulson. It's a little more—

Mr. Michel Coulombe: I don't remember exactly what I said. I remember saying "the envelope". I'm not sure if I said "nothing more".

Ms. Pam Damoff: It may not have been you, in fairness. I just remember the two of you trying to describe it. It could have been Commissioner Paulson at the time.

Mr. Michel Coulombe: What I'm saying is that I remember one of the two of us using that, that it's like the address on an envelope, nothing more, almost minimizing the importance of metadata, which certainly was not my intent, if I said that.

Ms. Pam Damoff: We've had a lot of testimony since then, and as well in another committee that I sit on, where we're looking at cyber-violence, that metadata is a lot more than that, and that you can actually get an awful lot of information from that associated data or metadata. I guess where I'm going with this is that you were collecting this information on innocent people for 10 years, and you still have it now. Is that right?

Mr. Michel Coulombe: Yes.

Ms. Pam Damoff: It's just not being accessed.

You've had the ability to share that information under Bill C-51. Was any of that information shared with other departments?

Mr. Michel Coulombe: The only information out of that metadata-associated data bank we would share is when we've done analyses and we can link a piece of that metadata to a threat.

Ms. Pam Damoff: Because SIRC only looks at you, not the RCMP and the other agencies. Is that right?

Mr. Michel Coulombe: Yes.

Ms. Pam Damoff: I'm just wondering whether any of that associated data was shared with other agencies that wouldn't have been subject to the SIRC review.

Mr. Michel Coulombe: No, we wouldn't share raw metadata with other agencies. As I said, we would only share it once we've made the link between that metadata and a threat-related activity.

Ms. Pam Damoff: I know there's been some discussion about whether or not the act needs to be changed. You're doing your own policies and procedures. One of the things we're looking at is making sure we're respecting people's privacy, while at the same time ensuring that Canadians are safe and secure.

Is there anything you could recommend that we could be putting in changes to the act that would help us to do this, or am I putting you in a difficult position?

Mr. Michel Coulombe: What I would say is the national security framework review that is ongoing is the place to have that discussion, because it seeks to achieve those two objectives: keeping the public safe and safeguarding our rights and freedoms.

The only thing I would add to this is that Judge Noël was clear on two points. One is that it was probably time to review the CSIS Act after 33 years, but also very important—because at one point someone mentioned the non-threat-related metadata and destroying it or not using it would have no impact on national security—Judge Noël actually acknowledged, after seeing the evidence, the usefulness of that program.

What people need to understand is that a piece of data that is non-threat related today could actually help us connect the dots or make links a year from now. I'm not arguing that, but all I'm saying is that before we make a decision, we have to have all the facts and really understand the potential usefulness.

Ms. Pam Damoff: I understand that. It was explained to me that it's like putting security cameras in someone's house all the time in case there might be a crime. People can relate to that.

I think when you're talking about data and associated data and metadata, it's like speaking a different language to people, but if you think of it in those terms, most people would say they don't want cameras in their house 24 hours a day just in case somebody might break in one day.

Mr. Michel Coulombe: I totally understand that. My point here is that I am telling you, from the other side, that it can be useful. The decision to keep it, use it, or destroy it because of privacy considerations is a public policy decision.

Ms. Pam Damoff: My time's up.

● (1715)

The Chair: Mr. Miller.

Mr. Larry Miller: Gentlemen, thank you for being here.

Mr. Coulombe, I want to continue on the potential eventual destroying of the data, but before I do that, I want to read one of your last paragraphs in your opening remarks. You said, "CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of non-threat-related associated data linked to third party communications collected under warrant."

Is any of this data stored or solely with the Department of Justice, or is it all within your department?

Mr. Michel Coulombe: No, it's all with CSIS.

Mr. Larry Miller: Okay, that's good.

Have you any idea with respect to timelines, when the decision to destroy or not destroy will be made?

Mr. Michel Coulombe: If I were going to give you a timeline...I can't at this point. It is a very complex decision.

Mr. Larry Miller: Would it be within six months, within a year?

Mr. Michel Coulombe: I would hope that within six months we would be in a position to decide what shouldn't be destroyed and what should be destroyed.

Mr. Larry Miller: That's fair enough. I realize that there are a lot of factors.

Now, let's say that the decision is made to destroy it. I want to go to a scenario back when the long-gun registry legislation was changed. It was eventually ordered that the data be destroyed. The order was made, and we were told that it was, but it was very obvious to many of us that, after the fact, I'll just say that some provinces or some individuals obviously had a copy of it, or part of it —we don't know. The reason I say that—and I can get the data or information to back this up—is that too many related instances on firearms about individuals came out when they went to renew...this kind of thing.

Once the decision to destroy this information is made, how can the average Canadian be 100% sure that it's going to be destroyed? I'm not suggesting that you would do otherwise, but sometimes there are a lot of people who have their fingers on the button, so to speak, Mr. Coulombe, and you're not the only one.

Mr. Michel Coulombe: That's a fair question.

That specific data bank is actually centralized in headquarters, and the number of people who have access to it to do the analytics is restricted. So, it's not accessible to all CSIS employees.

Again, SIRC has been tasked by the minister to monitor our response to the Federal Court decision. If and when the decision to destroy part of that data bank is made, I am certain that would be one aspect of, or reaction to, that decision that SIRC would review.

Mr. Larry Miller: Okay, just to carry it a little bit further, is it safe to presume that there's probably more than one copy of that information for safety reasons? It's like me renting a safety deposit box in a bank for important documents. Would the same kind of scenario apply to this case?

Mr. Michel Coulombe: Yes, we have backup of that data bank in the event that, for example, something would happen in headquarters, like some natural disaster. Again, the procedure is that if we were to destroy the data, we would make sure that the backup banks are also destroyed. Again, SIRC, I'm sure, would look at that.

● (1720)

Mr. Larry Miller: To close out, approximately how many people within the department would be involved in safeguarding that information, or at least have the ability to see it? Is it limited to two, three, ten? Do you have any idea?

Mr. John Cousineau: As Director Coulombe has pointed out, the one advantage we do have in being able to look at associated data is that it has been very much a centralized program. As Director Coulombe alluded, the information is within the walls of our HQ building, and we are very much aware of exactly where it is.

The exact number of users that we have in ODAC isn't actually representative of the folks who would see associated data because—as I return to my previous response—ODAC does more than just analyze associated data. Exactly how many people have access to the associated data? I'm going to put a number out there, but please don't quote me on it because it may be plus or minus a bit. I'm going to say probably twenty-ish.

Mr. Larry Miller: That's fair. That answers my question. Thank you very much.

Mr. Michel Coulombe: If you want, Mr. Chair, if that number is really incorrect, we can come back to the committee with—

The Chair: Thank you.

I'm just going to take my prerogative to ask one question. It follows up on Mr. Miller's question.

It's really for Mr. Frater about a concern that I have. I have read the judgment in the redacted version that we have as a public document, and Justice Noël's five principal decisions are quite clear and unambiguous. The government has decided to not appeal the decision and has accepted the decision.

However, CSIS depended upon the legal advice of Department of Justice officials. They went to the lawyers who are paid for by the crown and by the people of Canada to give the best legal advice. A Federal Court judge has unambiguously said that your advice was wrong. I just need to know what confidence you have, as the chief general counsel, in the advice you are giving the government on these important issues, and what steps you have taken to ensure that future advice on the interpretation of an act that's as important as the CSIS Act is correct.

Mr. Robert Frater: Clearly, we always strive to give the government the best legal advice that we can. In this situation, as in every other, we reviewed the case law, came up with the legal position, and ultimately the court disagreed with us.

The Chair: But it was over a 10-year period, from 2006 to 2016. That's a long period of time to be giving advice.

Mr. Robert Frater: It's not that we were giving wrong advice continuously over 10 years. There was a question of the legality of what it was that CSIS wanted to do. We gave an opinion on that, and until it's litigated, as it was here, we continue to believe that we gave the best legal advice based on the law as we understood it at the time. But from time to time it happens that judges disagree with us. Laws are struck down sometimes when Parliament thought they were constitutional. We might have given advice that in our opinion it was constitutional.

The Chair: Thank you.

Mr. Mendicino.

Mr. Marco Mendicino: I think in fairness sometimes judges of the Supreme Court have differing views on constitutional matters, but I digress.

At paragraph 204 of the October 4, 2016, Federal Court decision on an application for a warrant, I do not know if you have a copy of it handy, but there's one thing I would like to clear up so that I haven't misunderstood the testimony today. I'll read from that passage right now, which states:

> Presently, the CSIS must destroy [redacted] within a period of [redacted] from the time of collection, whether or not the communication has been assessed as threat related pursuant to condition 2 of the warrant.

That one sentence does suggest, unless I am reading it out of context, and sometimes context is difficult with redactions, that there is an expectation by the court that CSIS must destroy something within a period of time of collection. Can you provide some clarification about that?

● (1725)

Mr. Michel Coulombe: What you're reading is part of the new warrant conditions that we were proposing—and correct me, Rob—but it is basically going forward. When you read the decision, the judge didn't rule on what we have now in terms of destruction.

Mr. Marco Mendicino: I'm reassured to a certain extent by that clarification.

Mr. Coulombe, you did mention during your introductory remarks that there have been discussions between the service and the Department of Justice about how to improve co-operation and reduce the likelihood or probability of any concerns around candour with the court. Can you elaborate on how you see that co-operation strengthening going forward?

Mr. Michel Coulombe: In the Judge Noël decision, he does mention, in June 2016, the deputy minister of justice and myself appeared in front of the Federal Court en banc, so all available designated judges, to discuss the issue of duty of candour. As a result, we and the Department of Justice are now working on an action plan with a number of measures. We're waiting for the final reports with recommendations as to how to better discharge that responsibility, and obviously we'll report back to the court in terms of those recommendations.

Mr. Marco Mendicino: Do I have any more time, Mr. Chair?

The Chair: You have two and a half minutes.

Mr. Marco Mendicino: That's a rare occasion.

Can you take a few moments, then, since we have the time, and give us some specific examples about how you see this co-operation working?

Mr. Robert Frater: The main criticism in the judgment is about our breach of the duty of candour. I don't think there's any misunderstanding in the department or in CSIS that we have to do better. I think what the court is telling us is that for certain decisions that they're going to make, like the decision to issue a warrant, they want some more context, so we have to be careful that we are giving them enough context so they can make a proper decision. We have to make sure that all of our people are aware of that duty, both the affiants from CSIS and the lawyers presenting the case to the court. We are taking advice from outside experts on how we can do better by looking at best practices in *ex parte* matters in other jurisdictions.

Mr. Marco Mendicino: Have you learned anything specific in studying some of the examples from different jurisdictions on [*Inaudible—Editor*]?

Mr. Robert Frater: We're waiting for a final report from our outside experts on that question. Warrants under the CSIS Act are somewhat different from Criminal Code warrants. One of the things we've asked our experts to do is to look at what other people do in different contexts, but to look particularly at this context because it is something different, and we're trying our best to come up with a plan that recognizes the unique nature of these proceedings.

Mr. Marco Mendicino: Thanks, Mr. Chair.

The Chair: I thank the witnesses very much. You've answered our questions and have been helpful.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

PERMISSION DU PRÉSIDENT

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca

3103(93/01)

Follow-Up Response
The Standing Committee on Public Safety and National Security (SECU)
Regarding Supplementary Estimates B 2016-2017 and CSIS
Thursday, December 8, 2016

FOLLOW UP #1

Excerpt From Transcript:

Mr. Larry Miller (Conservative): To close out, approximately how many people within the department would be involved in the safeguarding or at least the ability to see that? Is it limited to two, three, or ten? Do you have any idea?

Mr. John Cousineau: As Director Coulombe has pointed out, the one advantage we do have in being able to look at associated data is that it has been very much a centralized program. As Director Coulombe alluded, the information is within the walls of our HQ building, and we are very much aware of exactly where it is.

The number of exact users we have in ODAC isn't actually representative of the folks who would see associated data, because—as I return to my previous response—ODAC does more than just analyze associated data. How many exact people have access to the associated data? I'm going to put a number out there, but please don't quote me on it, because it may be within plus or minus a bit. I'm going to say probably 20ish.

Mr. Larry Miller: That's fair. That answers my question. Thank you very much.

Mr. Michel Coulombe: If you want, Mr. Chair, if that number is really incorrect, we can come back to the committee with [Inaudible].

RESPONSE

The Canadian Security Intelligence Service's (CSIS) analysis of associated data is centralized with the Operational Data Analysis Centre (ODAC) at CSIS Headquarters. There are 21 data exploitation analyst positions within ODAC for the purpose of analyzing data to assist in answering operational questions that advance Service investigations. However, further to actions taken by CSIS following the Federal Court's decision, none of these analysts currently have access to any associated data that the Federal Court determined did not meet the standard for legally authorized retention.

It is important to add, however, that data, by its very nature, is held in information technology systems that are supported by information technology professionals. There are approximately 40 such employees that provide technical, programming, database, system security and administrative support for the overall systems in which the associated data is retained. They do not access the data for analytical or operational purposes.

Follow-Up Response
The Standing Committee on Public Safety and National Security (SECU)
Regarding Supplementary Estimates B 2016-2017 and CSIS
Thursday, December 8, 2016

FOLLOW UP #2

Excerpt From Transcript:

Mr. Matthew Dubé: Mr. Coulombe, I only have a few seconds left. Obviously, you don't have that information at your fingertips, but you can provide it to the committee. I am curious to know the numerical relationship between the number of people for whom you have the related data and the number of people who were the target of the investigations. I would like to know that proportion.

RESPONSE

While the Canadian Security Intelligence Service (CSIS) wishes to support the Committee's study of CSIS' data retention, access to the data has been halted in order to comply with the Court's ruling.

It is important to note however that associated data does not reveal the purpose of the communications, nor any part of the content, and does not identify individuals. As such, even if access was possible at this time, CSIS would regrettably be unable to quantify the number of individuals linked to the associated data.

The Service accepts the Court's ruling and efforts are underway to develop and implement policies, processes and technology to address the Court's decision.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 028 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, October 6, 2016

Chair

Mr. Robert Oliphant

Standing Committee on Public Safety and National Security

Thursday, October 6, 2016

● (1530)

[*English*]

The Chair (Mr. Robert Oliphant (Don Valley West, Lib.)): I'm happy to call to order the Standing Committee on Public Safety and National Security for this, our 28th meeting, as we study the national security framework.

We very much want to thank Minister Goodale for joining us today, as always. We also welcome the deputy minister, who is relatively new to the position. I believe it's your first time at our committee. You will find we're an excellent committee, as you will tell by our questioning and our knowledge of this subject.

We welcome the minister to give opening remarks. We have him here for the first hour of our meeting and officials will gather following.

Minister, you're on.

Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness): Thank you, Mr. Chairman.

Good afternoon, members of the committee. It's a pleasure to be back again. Thank you for the invitation to come on this occasion to talk about the consultations on the national security framework. I want to begin by thanking this committee for undertaking that study. It's an integral part of the government's approach to the future with respect to national security, and I'm grateful to have the committee's participation in the examination of that framework.

I also want to welcome Malcolm Brown. It's the first time he's had the opportunity to appear before the committee as deputy minister of public safety. I rely upon his good work and that of the women and men who toil in the department so faithfully to support the safety interests of Canadians.

In the second hour you will have the director of CSIS, Michel Coulombe, and the commissioner of the RCMP, Bob Paulson, in front of you. Those are always exceedingly interesting sessions. Even though he's not here at the table at the moment, I would like to acknowledge particularly Commissioner Paulson, who this morning made a historic announcement about a court settlement, and an apology and an approach going forward that will turn the page, we all hope, on a period of some considerable distress within the force having to do with harassment and sexual violence in the workplace. That announcement this morning was exceedingly important, and I congratulate all of those involved, including the commissioner, but also the very brave women who led that process over the course of the last number of years and had the patience, the persistence, the courage, and the perseverance to see it through to a successful conclusion.

Mr. Chairman, I want to thank this committee for its work in consulting with parliamentarians and with Canadians generally about Canada's national security framework. This helps to fulfill a commitment that we made to Canadians last year to give them an opportunity to have input on national security issues and to be as inclusive and transparent in that process as possible.

Before I wade into more details, let me pause for one more short detour, and that is to thank the committee for the report you filed earlier this week about post-traumatic stress injuries, which disproportionately affect first responders. Dealing with that challenge is another of my priorities on behalf of firefighters, police officers, and paramedics who work every day to keep the rest of us safe and secure. The committee's report was very well done, and it will be very helpful to the government as we bring forward a coherent national strategy for PTSI among our vital emergency response personnel across the country.

With respect to public consultations on Canada's national security framework, this initiative to have public consultations is absolutely unprecedented. We want to hear from parliamentarians, subject matter experts, and Canadians generally about how we can best achieve two overarching objectives. We need to ensure that our security and intelligence agencies are effective at keeping Canadians safe. Simultaneously, we need to be equally effective at safeguarding our rights and freedoms, and the open, inclusive, fair, and democratic character of our country.

I began this consultation work on this topic many months ago. We've collected important input from respected academics such as professors Wark, Forcese, and Roach, and from security and intelligence operators like Ray Boisvert, who was formerly with CSIS, and Luc Portelance, who was formerly at the CBSA and before that at the RCMP. I've also heard from former MPs like Bob Rae, Anne McLellan, and Irwin Cotler, as well as former senators Hugh Segal and Roméo Dallaire. I've met with a number of other current MPs and senators, and with outside groups like the B.C. Civil Liberties Association, OpenMedia, various organizations representing Muslim lawyers and other professionals, and many more.

That's a good start, but my direct meetings are going to be ongoing because the consultation is ongoing, and that is now augmented by the active and very welcome outreach by this committee.

● (1535)

More broadly, we have launched, as of last month, an online public consultation, and it will be running until the first of December.

By way of background, in the summer the government published its "2016 Public Report On The Terrorist Threat To Canada". That report covered the period through 2015 and into the beginning of 2016, highlighting the particular threat posed by individuals or small groups of lone wolves who get inspired to violence in some perverted way by the insidious influences of organizations like al Qaeda and Daesh. The threat report also included for the first time a description of Canada's national terrorism threat level. That level, by the way, is currently set at medium, where it has remained unchanged since October 2014.

To begin our online conversation with Canadians last month, the Minister of Justice and I posted a discussion paper and a backgrounder on our website. These do not purport to be statements of government policy. They are intended to elicit ideas and to provoke engagement on national security, and they certainly seem to be achieving that effect. Thus far, more than 8,000 responses have been received, with nearly two months yet to go in the consultation process. As I said, this online consultation will run until the first of December.

Whether it's our discussion with subject matter experts, or your committee work in talking to experts as well as other parliamentarians and Canadians generally, or the input we are getting online, we're looking for two types of advice: how we can enhance the effectiveness of our security agencies, and how we can equally and simultaneously safeguard our rights and freedoms, our open, inclusive, democratic society, and our Canadian way of life. These two core themes underpin our entire national security agenda.

On that point, I have noticed, of course, the report last week, and the committee appearance this week, of the Privacy Commissioner about the sharing of information. I consider Mr. Therrien to be a key part of the parliamentary oversight and accountability apparatus. I take his input very seriously, and I have already had one discussion with him about the points he raised in his report, and others will follow. In the meantime, in response to his point about privacy impact assessments in various government departments, I am now writing to all of my cabinet colleagues to ensure that all departments and agencies have in place the right privacy-related protections to deal with the issue of information sharing.

To close this introduction, Mr. Chairman, let me put these national security consultations in the context of our overall national security agenda as a government. That agenda includes the following points:

One, there is the creation of that new committee of parliamentarians that is reflected in Bill C-22, which you will have before you for consideration at another time. That is a cornerstone piece to bringing a brand new element into our oversight, scrutiny, and review architecture that has never before existed in Canada, but which has been recommended on a variety of occasions, by parliamentary committees, by the Auditor General, by external independent inquiries, and so forth. Bill C-22 will remedy the defect of that deficiency.

Two, we are hard at work on a new office of community outreach and counter-radicalization. The money for that was provided in the budget, and we're in the process now of identifying the individuals who will be best placed to deliver that new initiative.

Three, we will ensure faithful compliance with the Canadian Charter of Rights and Freedoms.

Four is clarity with respect to warrants.

Five is a more precise definition of propaganda.

Six is repairs to no-fly lists, and in particular the appeal process that relates to the no-fly list.

Seven is full protection of the right to protest.

Eight is a statutory review, after three years, of our anti-terrorism legislation.

● (1540)

Nine is a new arrangement with the United States with respect to our common border, including a much improved pre-clearance system and the establishment of an entry/exit data collection mechanism for the first time, as well as other improvements in the arrangements with respect to no-fly lists.

Ten is, and for the first time, this process. Canadians are actually being thoroughly consulted about what other steps, in addition to what I've already mentioned on the agenda, they believe are necessary to keep them safe and to safeguard our rights and freedoms.

Thank you, Mr. Chairman.

The Chair: Thank you very much, Minister. That was thorough and helpful.

We're going to begin our seven-minute round of questioning with Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you both, Minister Goodale and Deputy Minister Brown, for being here.

I wonder if I can take the opportunity in going first in the questioning to ask a couple of stage-setting questions.

Another committee I serve on is the Standing Committee on National Defence. That committee, in the context of a review of North American aerial readiness, received testimony that the single biggest threat to Canada is domestic terrorism. I'm wondering, drawing on the 2016 reports that I've read with interest on the terrorist threat to Canada, if you could tell the committee whether, or to what extent, you agree with that, whether that's too simple a conclusion from your perspective, or whether the threat is more multi-faceted than that.

Hon. Ralph Goodale: The threat is certainly multi-faceted, and it comes in many ways. Identifying the threat of terrorism, and in particular the inspired lone wolf, I think is identifying one of the key areas upon which we need to concentrate our efforts.

The threat report that was published in the summer indicated a number of things that seem to be new or evolving in the structure of threats that are affecting Canada. One of those is the advent of new technology that is changing all the time. Another is actually the gender makeup of some of the threats that we deal with and an increasing presence of women in the matrix.

Still, at the moment—and Director Coulombe would be able to give you a good deal of texture with respect to this analysis—one of our key concerns is those lone wolves who are on the Internet or who somehow get inspired by al Qaeda or Daesh and get on a path to violent behaviour. That's why we have a particular focus on the counter-radicalization initiative, to try to put ourselves in a position to identify that risk in advance and, to the extent we can, head it off.

● (1545)

Mr. Sven Spengemann: I'm wondering, to add briefly to that, if you could tell the committee generally, because I'm assuming there are classification levels involved here, the extent to which the threat level varies with the intensity of commitments by our armed forces abroad and in other missions, whether military or peacekeeping, or other exercises in the Middle East and central Asia. In other words, to put it in very simple terms, does the threat increase the more we do abroad?

Hon. Ralph Goodale: Obviously, I need to be careful in answering that question because, as you say, classified information is involved. One of our leading priorities is to make sure that when Canadians are in harm's way, they are properly protected to the maximum extent possible.

Mr. Sven Spengemann: That's helpful. Thank you, Minister.

The second line of questioning draws on a line from the "2016 Public Report On The Terrorist Threat To Canada". It talks about building a safe and resilient Canada. My colleagues will take you into the details of the mechanisms that you're proposing on the national security framework.

I'm wondering if you could talk a bit about the role of Canadian society with respect to good security and good safety. I'm particularly interested in how Canadians perceive national security in 2016 and what their role is. The fact that you itemized consultations as a very important part of our commitment will bring Canadian society into the discussion.

What is the role of Canadian society in not only preventing attacks but also making us socially resilient? If that's the right path to go down, how important are relationships not just between communities and government, but also between communities with respect to counter-radicalization and tackling the misperceptions and distortions that are imbedded in the term "terrorism"?

Hon. Ralph Goodale: That's not only important in terms of our national security, but it's also an instinctive part of the character of Canadians, I think, to want to build that sense of cohesion.

We're a country that is extraordinarily diverse. I think it was the Aga Khan who said that Canada is the finest example of pluralism the world has ever seen. That's a great compliment. He is an honorary citizen of this country, and we take that compliment very sincerely and gratefully. But in that diversity, you constantly have to work at social cohesion. That involves reaching out to each other and understanding one another, trying very hard to build bridges with each other. The kind of country we have and the kind of history we have hold us together, not so much by the force of law or the force or arms, but by our common will. We're a successful country because we want to be, not because we have to be. You have to keep promoting that sense of common cause, understanding, and outreach.

This consultation is intended for two purposes. One is to let Canadians have their say, and they've wanted to have their say for a long time. This is the first time in history that they're going to get it, so they're participating in the process. Also, by listening to the conversation, whether at this committee table, online, or in the other rooms in which the consultation is taking place, hopefully we'll elevate the level of understanding about what national security means, what the framework is, and what the threat level is, and reinforce the point, too, that fundamentally we are a safe and peaceful country. We need to make sure we keep it that way, but Canada is in a very privileged position in the world.

● (1550)

Mr. Sven Spengemann: Thank you, Mr. Chair. I'll leave it there. I'll delegate the rest of the time to the next Liberal speaker.

The Chair: Mr. Miller.

Mr. Larry Miller (Bruce—Grey—Owen Sound, CPC): Minister, thanks again for being here. It's always great to have a minister at the committee.

I want to talk about the new powers that were granted under Bill C-51 to CSIS. Basically, it gave them new powers to disrupt potential threats. There are different things, telephone calls, travel plans, etc. Before the changes in Bill C-51, CSIS could only inform police agencies of potential threats and could not act on them alone. Throughout the last election campaign, Mr. Minister, your party basically said they were going to make major changes to it.

Now, the director of CSIS appeared before a Senate committee in March. He indicated that the agency had used their new powers close to two dozen times since Bill C-51 came into force and six more months have passed since then. He also indicated that it is likely that they'd use these powers again in the future. During an interview following being at the Senate committee, the director of CSIS stated that, following the national security review that the government is currently engaged in, a decision would likely be made that could affect the power and others.

Mr. Minister, seeing that if the powers that be would have had the proper things at the time, Corporal Cirillo probably would still be alive.... We were all here two years ago when that happened, and I'm sure you were as well. Also, the would-be terrorist, I believe, in Strathroy a few months ago probably wouldn't have been caught without these new changes.

My question is, do you intend to change them, and if so, how do you see these powers changing? Clearly, they've been effective in disrupting potential threats thus far.

Hon. Ralph Goodale: Mr. Miller, thank you for your greeting.

On the threat reduction activities, that is one area where we want to listen very carefully to Canadians' views, because views are mixed on that power. If you remember, the original creation of CSIS flowed out of a decision by a previous government to remove intelligence functions to a significant extent from the RCMP and hand them over to an independent agency that would specialize in intelligence, while the RCMP would deal with policing issues. There was a policy decision at that time to separate the two functions. Now, many years later, the legislation was changed to, in some ways, merge them back together again. I think we need to think carefully about that.

Mr. Larry Miller: Do you intend to change them, Mr. Minister?

Hon. Ralph Goodale: The commitment that we made in the platform was to ensure compliance with the Canadian Charter of Rights and Freedoms.

Mr. Larry Miller: Of course.

Hon. Ralph Goodale: That was the commitment that was made. There was language in Bill C-51 that tended to contradict that, so that is the issue that needs to be addressed—

Mr. Larry Miller: Okay, Mr. Minister.

Hon. Ralph Goodale: —compliance with the charter.

Mr. Larry Miller: I'm running out of time.

You really haven't said whether you are going to change them or not, and how would that look if you do. The answer to one is a very quick yes or no, and with the other one, if it's yes, then how?

Hon. Ralph Goodale: The point is, Mr. Miller, why would you have a consultation if you've already determined the answer to the question?

As I said at the beginning of my answer, we want to hear from Canadians on this subject. The bottom line for us is compliance with the Canadian Charter of Rights and Freedoms.

Mr. Larry Miller: Okay, did you consult, then, prior to making that announcement during the election? I think that we know—

Hon. Ralph Goodale: What announcement? We announced compliance with the charter. That's what we announced.

Mr. Larry Miller: Yes, well it goes beyond that, I think.

Hon. Ralph Goodale: Well, that may be your platform; it's not mine.

Mr. Larry Miller: Well it was your party that said it, so—

Hon. Ralph Goodale: No, we didn't. Read the platform, page 55. I'm happy to send you a copy.

Mr. Larry Miller: I'm going to move on here.

We all know, and in fact you even said, that organizations have used the new power. Citizenship and Immigration Canada, the CBSA, CSIS, and a fourth unnamed agency have used these.

It's obvious, Mr. Minister, that the changes have been used, and I'm sure they wouldn't have been used unless they were a valuable tool, so—

● (1555)

Hon. Ralph Goodale: You've segued from one power to another. You've segued from threat reduction activities, which was the subject of your first question, to information sharing, which is the subject of your second question.

The two are quite different subjects.

Mr. Larry Miller: Okay, that's fine. I wasn't getting much of a response to the other, so I moved on.

On that, are you going to change the information-sharing process? Obviously these organizations are saying that they're using it, and it seems to be working.

Hon. Ralph Goodale: In respect of that new piece of legislation which was introduced as a part of Bill C-51, in my remarks today I said that the Privacy Commissioner has indicated his view that there are some defects in the process, including whether privacy impact statements have been properly prepared and so forth.

What I've undertaken today, further to my conversation with the Privacy Commissioner a few days ago, is that I will be in touch with every minister in the cabinet to make sure they have the systems in place that will properly respect and protect privacy.

Mr. Larry Miller: Just to carry this out, a number of people, and I'll even go to my own personal.... I'm a private person. I want my rights protected, and I want all Canadians' rights protected. However, we live in a different world today, Mr. Minister, than we did even 10 years ago. What I mean by that is the threats that are out there. Mr. Spengemann talked about domestic terrorism. There is no doubt it's more prominent today than ever.

It comes back to this. I like my privacy and I think most Canadians do. At the end of the day, I find it a small sacrifice...if our agencies that protect us all have tools to actually do the job.

Also, if I have done nothing wrong, I have nothing to worry about. I've had that said to me. I'm sure you've had some of your constituents tell you that. How do you respond to that?

The Chair: Thank you, Mr. Miller.

[*Translation*]

We continue with Mr. Dubé.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

Thank you for being here, Mr. Minister.

I want to talk about your election platform. Before me, I have a passage that lists the changes that will be made. After the list of those measures, we read the following: "As this legislation is tabled in Parliament, we will launch broad public consultations, to engage and seek the input of Canadians and subject-matter experts." We had understood that the bill was going to be introduced and that Canadians would then be consulted. But no, they are being consulted beforehand. Meanwhile, very serious breaches are being raised, including by the Privacy Commissioner, and the problems are not being solved. Those powers continue to be used with no adequate oversight.

What will happen next? Are you going to introduce a bill to make changes to the provisions in Bill C-51 and then consult again?

Why not stand by the commitment in your platform, to introduce a bill with the measures you are proposing, and consult afterwards?

Clearly, your mind is already made up. You have just listed the measures that correspond exactly with your election platform.

[*English*]

Hon. Ralph Goodale: Mr. Dubé, the fundamental cornerstone commitment that we made in the platform was to create the new committee of parliamentarians. That piece of legislation is now before Parliament, and it will undoubtedly be thoroughly analyzed by this committee and by the public in the process.

There are several other commitments in the platform. It may well take two or three different pieces of legislation to work our way through all of them, but we are moving in a very measured and logical way to deal with the defects that we found in Bill C-51 , to bring this whole new architecture, including the committee of parliamentarians, and in the process, to give Canadians the chance to be heard which they were denied—

● (1600)

Mr. Matthew Dubé: Minister, you understand that my time is limited. There are seven bullet points on the Liberal Party website where you have committed to fixing Bill C-51 . In the paragraph at the end of those bullets—and only one of those bullets mentions the oversight committee—there's a specific mention that you'll consult Canadians after presenting legislation, which has not been done.

The concern I am raising, which I think is very serious especially in light of the Privacy Commissioner's report, is that these powers continue to be used. The problems have not been fixed. This committee has not been put in place over a year into your government's mandate, and I understand the bill is moving through the House. That's fine, and there are problems with that, and we'll get to those. But why is there no legislation, and how can we trust these consultations when, beyond the criticisms that have been raised by the Privacy Commissioner and others we've heard from, there's already a list that was committed to in the election and that you yourself just enumerated in your presentation?

Hon. Ralph Goodale: As I said, the cornerstone piece of legislation is in the public domain. There are also two others that I would point to that deal with cross-border issues with the United States. That legislation has been prepared and published. We are now conducting the necessary consultation in addition to having the list of specific things that I mentioned to ask Canadians the key question of whether there is something else they want included or they think is valuable to be included in the reform package to accomplish two objectives: keeping Canadians safe and making sure that our rights and freedoms are safeguarded.

This is a process we began to work at immediately after the election. It's a huge, complex area. We're going at it in a thorough and logical way. I might also point out that the reason previous governments got into jackpots on these issues is that they tended to scribble down policy on the back of an envelope and didn't do the proper consultation in advance.

Mr. Matthew Dubé: You voted for that policy though. That's what I don't understand.

[*Translation*]

The commissioner's report indicates that the definitions and the thresholds are problematic. Those are the points that have been raised. The commissioner could have made the same presentation that he made on Tuesday in the last Parliament and his comments would have been the same.

We are very concerned about the consultation process. You start the ball rolling and then you start it rolling again. This is serious; the rights and freedoms of Canadians are in danger. We can hear it and we can see it. Meanwhile, those powers continue to be used. We see the shortcomings and there is no solution.

How do you respond to the commissioner and to others who are saying that the process, the green paper, seems to focus only on law enforcement organizations and not at all on the protection of privacy? A lot of experts are saying that. If we read between the lines, it seems that we have already come to the end of this process.

[*English*]

Hon. Ralph Goodale: No, I beg to differ, Mr. Dubé. The process is not by any means being pre-empted. In a sense, your argument is a bit contradictory, because you're saying "introduce legislation and consult later"—

Mr. Matthew Dubé: I'm just asking you to respect your election commitments. We want it to disappear. We want to repeal Bill C-51 .

Hon. Ralph Goodale: —while I'm saying that the core piece of legislation has been introduced. It's Bill C-22. There will be perhaps two or three other bills that will come later on, obviously the ones dealing with the specific commitments in the platform, but it is useful to ask Canadians what else they want to see considered. Indeed, the Privacy Commissioner's items are not included in the list of the first seven, so the consultation has already yielded results by bringing forward his perspective on that particular issue.

Other people have said that we need to deal with the deficiencies in peace bonds. That is a critical deficiency as well, and we learned in the Strathroy case that the peace bonds that were described a couple of years ago as being a kind of panacea solution aren't, and they need to be fixed.

Mr. Matthew Dubé: Many say part of the problem there is that police don't have resources, and that the reality is Bill C-51 wasn't even necessary because if law enforcement actually had the resources and if there actually were a counter-radicalization strategy, we wouldn't even be debating Bill C-51 now, and that those are the actual tools that would really make a difference.

Do you agree with that?

Hon. Ralph Goodale: We're moving on all of those fronts.

Mr. Matthew Dubé: It seems like we're consulting a lot, but you have specific proposals. How can you convince Canadians that it's not already a foregone conclusion when, right on the Liberal website, it's there?

Hon. Ralph Goodale: Those specific proposals are the minimum we will do in the changes to legislation. What we're asking Canadians in the consultation is what else they think needs to be added to that list.

Canadians have already added to the list. They've added issues around privacy. They've added issues around peace bonds. In the 8,000 submissions we've had, they've added a good many other ideas as well. It's useful to ask Canadians what they think, because they'll always give useful information.

● (1605)

[*Translation*]

Mr. Matthew Dubé: Thank you.

[*English*]

The Chair: Thank you, Minister and Monsieur Dubé.

[*Translation*]

Next we have Mr. Di Iorio.

Mr. Nicola Di Iorio (Saint-Léonard—Saint-Michel, Lib.): Mr. Minister, thank you for your remarks, for the preliminary announcement you have made, and for taking the time to meet with us.

First of all, could you list the dangers that Canadians should be on guard against? You have talked of one danger in particular. I understand that it can vary by region. However, would it be possible just to indicate some of the other dangers that threaten Canadian society?

[*English*]

Hon. Ralph Goodale: Mr. Di Iorio, I would refer you broadly to the threat assessment report. That goes through in detail where we feel the principal threats are located.

As I said, the key one is the inspired lone wolf. They are perhaps the most difficult to defend against, because they tend to act in isolation. If a terrorist organization is plotting some grand scheme, for example, the attack on Paris almost a year ago, an enterprise like that tends to involve a sufficient number of people and a significant amount of planning activity and tends to leave tracks. Evidence can accumulate. In the case of the lone wolf, there's not that kind of activity. They tend to be isolated. They're not using sophisticated weaponry. They're still dangerous, however, as we saw in Strathroy this summer, a prime example of that kind of problem. It can happen all across the country.

[*Translation*]

Mr. Nicola Di Iorio: Mr. Minister, one major concern is the dilemma faced by Canadian society. On one side, we have people who want to do us harm, who want to commit acts of violence against Canadians. On the other side, we have the forces of law and order, which are in place to prevent that danger from occurring. The dilemma is that, by their very nature, the evildoers, who want to commit acts of violence, do not inform the public about the evil, the violence, that they are preparing to commit. So we cannot know what they are preparing to do. On the other hand, the forces of law and order do not want to disclose the nature of their investigations in order not to prejudice those same investigations.

Could you enlighten the committee on how we navigate through this dilemma when we have to properly inform Canadians about the dangers they face?

[*English*]

Hon. Ralph Goodale: Part of it can be through a consultative process like this one.

Part of the answer is making sure that our security and intelligence and police agencies have the right kind of independent oversight. We'll be adding to that through the committee of parliamentarians, but already, there is oversight provided in most cases, but not all. That's another issue we need to address in this consultation process: where there are gaps in the oversight mechanisms, for example, with respect to CBSA which does not have an agency providing oversight like SIRC provides to CSIS, or the CRCC provides to the RCMP, or the commissioner provides oversight to the communications security establishment in National Defence.

If you read the reports of those agencies.... SIRC just published its report a week ago. It is a very interesting overview of CSIS' activities in the last fiscal year. It shows the kinds of things that they've been looking into, the kinds of activities they've been conducting both in Canada and abroad, and where the activities of the agency could potentially be upgraded.

This oversight function, I think, can be very helpful to the public in understanding what the agencies are doing, and that in the process, they are effective and they are safeguarding Canadian rights and freedoms. I would commend to you those detailed reports by the oversight agencies. Ultimately, when we add the committee of parliamentarians, that overview which will come at least annually from a committee of nine parliamentarians will add another dimension to Canadians' ability to understand what our various police, security and intelligence operations are doing.

● (1610)

[*Translation*]

Mr. Nicola Di Iorio: Thank you, Mr. Minister.

Canada is a federation, so constitutional powers are shared and legislative powers are shared. You mention the exchange of information between federal agencies. How can we be assured that provincial agencies and authorities also share information between themselves and with federal authorities?

[*English*]

Hon. Ralph Goodale: Our jurisdiction is federal, so we have to be careful to respect the Constitution in that regard, but there is very effective co-operation among all levels of police forces in the country.

To go back to the incident on the 10th of August in Strathroy, Ontario, the first people to be notified, of course, were the RCMP, but as they went about identifying the individual, Aaron Driver, and his location, they engaged the city police force in London, the regional local community police force in Strathroy-Caradoc, and the Ontario Provincial Police.

The federal, provincial, and two municipal police forces collaborated very effectively together. It was a seamless operation. We could actually add a fifth level to that because the original information came from the FBI in the United States. That was a classic illustration of how our various forces and agencies communicate with each other and co-operate with each other to make sure that we're keeping Canadians safe.

The Chair: Thank you, Minister.

[*Translation*]

We continue the second round with Mr. Brassard.

[*English*]

Mr. John Brassard (Barrie—Innisfil, CPC): Minister, thanks for being here today.

Yesterday, *The Globe and Mail* reported that you said recently that Bill C-22 creates a committee that "will set its own agenda and report when it sees fit." Yet an independent report by the Library of Parliament stated:

> How much the committee members would be able to access state secrets is in question because the legislation would allow cabinet ministers to block reviews of some spy programs and thwart the committee's bids to see sensitive documents. "Bill C-22 authorizes ministers to refuse to provide information."

We know there are seven exemptions that are in place within the legislation. We also know there was an issue back in 2010 where Speaker Milliken ruled on a question of privilege. He was quite clear in his ruling that the fact that there was sensitive information, or intelligence documents, or information relating to an ongoing investigation did not remove the obligation of the government to share those documents with the House. In fact, you said in support of that ruling, "That series of questions of privilege resulted in your ruling on April 27, when, in very eloquent terms, you indicated that Parliament did have the right to information."

As a committee of Parliament, what has changed, Minister?

Hon. Ralph Goodale: If you read the entire judgment from Speaker Milliken, you'll see that he put national security—

Mr. John Brassard: —national defence, international relations—

Hon. Ralph Goodale: —protections in place in the very structure of his ruling.

The point is this. With the greatest of respect to the author of that report from the Library of Parliament, I would disagree with his conclusions. I know we're not discussing Bill C-22—

Mr. John Brassard: May I ask you, then, Minister—

Hon. Ralph Goodale: Just a second. I want to answer your first question before you go on to a second one.

● (1615)

Mr. John Brassard: I want to ask another question, so be brief.

Hon. Ralph Goodale: Well, if you want an answer to the question, it takes a little time.

Bill C-22, which I gather we are discussing today, Mr. Chair, even though we weren't supposed to be—

The Chair: We'll try to keep Bill C-22 to a minimum, and we estimate that we will be having you back on Bill C-22 in a few weeks.

I'll give you extra time because I've taken your time, but let's try to keep Bill C-22 down to a minimum.

Hon. Ralph Goodale: Bill C-22 provides to this Canadian committee of parliamentarians more authority, more scope, and more power than almost any of its counterparts in any of our allied countries. It will have more jurisdiction to provide a higher level of oversight, and the intervention of a minister or the Prime Minister is limited only to those cases where a particular review at a particular point in time would be injurious to national security. On those grounds, a minister or the Prime Minister could intervene to say, "Not this particular area at this moment in time". They would have to give written reasons to the committee as to why they were making that judgment.

Mr. John Brassard: May I ask, Mr. Chair, how much time we have left?

The Chair: You have another two minutes.

Mr. John Brassard: Okay.

When you say that it will set its own agenda and report when it sees fit, what do you mean by that?

Hon. Ralph Goodale: It can look at any activity in the Government of Canada. It can ask for any information within the Government of Canada. It is required by the draft statute to report at least once a year. It's entitled to report at any other time that it thinks is appropriate. If this committee finds something in the national security activities or architecture of the government that it thinks is wrong, either not effectively keeping Canadians safe or not respecting Canadians' rights and freedoms, then the committee is perfectly at liberty to blow the whistle.

The committee cannot divulge classified information, and I presume no one around the table would argue that it should. Classified information needs to be classified. But if members say publicly—and if you have seven MPs and two senators, it's certainly going to be public—that something here is wrong, even without divulging the classified detail, they can blow a whistle that will make it exceedingly uncomfortable for the government of the day. That whistle will keep being blown until the problem is solved. They have a bully pulpit like no other.

Mr. John Brassard: Thank you, Minister.

The Chair: Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thank you for appearing, Minister.

I'm going to start with the simple premise that when we limit Canadians' rights, we have to justify that those limits are necessary. I want to speak to the threat reduction powers specifically. Can you speak to the necessity for these powers? What was wrong with the previous regime, and why are these reduction powers necessary?

Hon. Ralph Goodale: Mr. Erskine-Smith, that's exactly the reason that we're having the consultation—

Mr. Nathaniel Erskine-Smith: Fair enough.

Hon. Ralph Goodale: —because we want to hear Canadians on this topic. They didn't have a full opportunity to be heard before. We're giving them that opportunity now.

Mr. Nathaniel Erskine-Smith: That's absolutely fair. In the interim, while consultations are ongoing, I recognize that obviously you've restricted the ability of CSIS or CSIS has agreed to not seek a warrant to violate charter rights. However, there have been dozens of opportunities, if not more, of CSIS engaging in threat reduction powers. What assurances can we give to Canadians that their rights are being protected in the interim?

Hon. Ralph Goodale: The report from SIRC, the Security Intelligence Review Committee, tabled last week indicated that not only had no threat disruption activity that would have required a warrant been undertaken, but also that no warrant was even asked for.

Mr. Nathaniel Erskine-Smith: There are threat disruption activities that have been undertaken without a warrant, and so those threat disruption activities presumably—

Hon. Ralph Goodale: —are completely consistent with the law and completely consistent with the charter.

Mr. Nathaniel Erskine-Smith: They are reviewed—

Hon. Ralph Goodale: —by SIRC. Indeed, one of the requirements of the Security Intelligence Review Committee is to review those activities every year, and that may be one thing that the new committee of parliamentarians would want to delve into on a regular basis, as well.

● (1620)

Mr. Nathaniel Erskine-Smith: It's a good segue to the issue of oversight. The RCMP, CSIS, and CSE are each subject to oversight, or review bodies, I should say. CBSA, you noted in response to a previous question, is not. Quite a bit of the academic literature suggests that we have a silo effect. We have whole-of-government security, but we don't have whole-of-government review. I wonder if you could speak to the necessity of whole-of-government review and your experience to date.

Hon. Ralph Goodale: That's a very good point and a very good question.

One of the virtues of the way we have structured the committee of parliamentarians is that it is not in any silo. When the British review mechanism was established, for example, there were four specific agencies that the British committee could look at; no others, just four. In the Canadian model, we have made it government-wide. This committee will have, first of all, access to classified information that has never before been made available to parliamentarians. Second, they can follow the information wherever it leads, from agency to agency and department to department. Wherever it goes in the government, they are entitled to look at all of it.

Mr. Nathaniel Erskine-Smith: Without getting into Bill C-22 and parliamentary oversight, but specific to expert review, the academic literature suggests that in addition to parliamentary oversight and review, and in addition to the three review bodies, a super-SIRC is likely necessary. Would you speak to that, specifically?

Hon. Ralph Goodale: That is an idea I want very much to examine in this consultation process, because there are gaps in the architecture. You pointed that out, as I did, with CBSA, and there are others. You need the expert analysis, and you need the parliamentary analysis. Since we've never had the parliamentary analysis before, there will be some working out here of how the two interconnect with each other, but both are required, and we have to find a way to get out of the silos.

The parliamentary committee by definition is out of the silos. The review bodies below them are still limited, and we'll have to examine how you get that cross-fertilization.

Mr. Nathaniel Erskine-Smith: I have one final question with respect to information sharing. The Privacy Commissioner attended before another committee I sit on, which is the privacy committee, and suggested that he was not completely clear on how much information had been shared under the new act.

The departments hadn't all been completely forthcoming in a timely manner with his office. I wonder if you could give some assurances to Canadians that you're seized with this matter.

Hon. Ralph Goodale: Yes. I was concerned with the Privacy Commissioner's comments. As I said earlier, I consider him to be an essential part of the oversight apparatus, and I take his advice very seriously. As a first step, I'm in the process of writing to all of my cabinet colleagues to remind them of the obligations that are imposed on departments by virtue of the new legislation and to make sure that they have the right privacy protections in place.

The Privacy Commissioner is usually very forthcoming in providing advice about what he thinks is necessary to fix problems.

The Chair: Thank you, Minister.

[*Translation*]

We now move to Mr. Généreux.

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

Mr. Minister, thank you very much for being here today.

As you know, we have already started the consultation. The green paper serves as the working document for the consultation. In addition to the Privacy Commissioner, we heard from another witness this week, Professor Wark, who stated that the green paper understates the whole digital aspect of national security.

Allow me to paraphrase your leader: it's 2016. In my opinion, this aspect is extremely important. We cannot underestimate the threats that can be made against Canada, especially not from the social and digital media that can attack our security.

I would like to know what you think about it. As you signed the green paper, I imagine that you are well aware of it.

[*English*]

Hon. Ralph Goodale: There are three different consultations going on with respect to cyber issues and digital issues. Obviously, that is included, in part, in the national security review that I am responsible for. At the same time, we have a focused discussion with industry and with the public on cybersecurity issues and the protection of critical Canadian infrastructure. That's going on at the same time in a different forum, a parallel study. In addition to that, cyber issues are covered in the national defence review that my colleague the Minister of National Defence is conducting.

It's a crosscutting issue. It's not just in one department or one dimension of government. Cyber issues cut across the whole span of government and the private sector operations. It's a field that is rapidly evolving, and we need to make sure that our cyber policy is up to speed. The last cyber policy in Canada was from 2010, I believe. Even in the span of four or five years, it is generally regarded now as outdated. It was thought to be, in 2010, quite avant-garde, ahead of the curve, but cyber issues have evolved so dramatically that we are not as up to speed as we ought to be. That is why we are looking at it from the point of view of public safety, from the point of view of industry and the private sector, and from the point of view of national defence.

● (1625)

[*Translation*]

Mr. Bernard Généreux: In our study, do you want us to focus on anything in particular in order to learn any specifics in the area of public security in the committee's purview? Would you like to see some aspects more than others in our final report?

[*English*]

Hon. Ralph Goodale: There are a huge number of issues you might tackle, but one, which is referred to in the paper, is the phenomenon that police and security agencies call "going dark", when the activities of would-be criminals or would-be terrorists are so technically encrypted from beginning to end that there is no ability, or very limited ability, to detect the activities of those who would pose a threat to public safety or national security. That issue—

[*Translation*]

Mr. Bernard Généreux: Do you know whether terrorist organizations are able to do that? What do you understand by "going dark"?

[*English*]

Hon. Ralph Goodale: That's the buzz phrase, "go dark". This means that, if you are an investigator, all of a sudden all of your access to information evaporates, because not only the material but the systems that carry the material are so heavily encrypted you are not able to even detect the trail that you might like to follow. That is a huge issue that is technological on one side, and legal and constitutional on the other side. It would be very useful to hear the debate in the committee and the evidence of the witnesses you might call, to delve more deeply into that very critical field. It's a field that had a bearing on the ability to detect, or not, the activities of Mr. Driver.

The Chair: Thank you, Minister.

We are almost at our time. We have one questioner left.

I can give you about a minute and a half.

Mr. Marco Mendicino (Eglinton—Lawrence, Lib.): Thank you, Minister. It is always good to see you at committee, and I want to commend you for leading Canada's first-ever public consultation on national security. It's truly historic.

I have time for one question, and I want it to relate to counter-radicalization. Can you tell this committee what, if any, partnerships you see with social media outlets like Facebook, Twitter, and Instagram, where there is, sadly, regrettably, a lot of non-sanctionable speech that crosses the Rubicon into inciting terrorist activity? What kind of partnerships do you see going forward so that we can stymie the spread of that?

● (1630)

Hon. Ralph Goodale: The whole effort in terms of community outreach and counter-radicalization will need to be built on partnerships. The federal government can establish a centre of excellence, pay for research, and promote coordination and co-operation, but the actual activity that will make a difference in heading off that cycle into violence will be at the community level, with religious and social organizations and with the private sector, such as those who are very good at communicating.

We are going to have to consult with them very carefully to get their advice about the right way to intervene and the right message that intervenes most effectively with the right people at the right time at the right place in order to head off a tragedy. Partnerships with community organizations and with private enterprises that have expertise in this field will be absolutely critical.

Mr. Marco Mendicino: Thank you very much, Minister.

The Chair: Minister, thank you for your time with the committee.

We expect to see you in a few weeks. We have the honour of having your deputy staying with us as other officials come in.

Let's take a moment as we pause and let the minister leave and other witnesses come in.

● (1630)

(Pause)

● (1635)

The Chair: Committee, I know you'll be very pleased that we're going to get right to questioning. The opening statement was done by the minister, and we now have witnesses here.

Mr. Brown from the department is still here. He is now joined by Ms. Beauregard.

Monsieur Coulombe, from CSIS, welcome again.

Mr. Paulson, it's nice to see you back.

Thank you for taking the time to join us.

As you know, we are beginning a fairly large study of the national security framework. This is not a legislative study. It is a study by parliamentarians on the whole framework, which we hope will help to advise the minister as he considers both policy and legislative changes in the coming year. That is the nature of our work. We're not dealing with any legislation in particular. We will be dealing with Bill C-22, now that it has been referred to us. If Bill C-21 and Bill C-23 pass in the House, we expect they will also come to us. This is really very much at the theoretical level of what we as parliamentarians need to be advising the minister on, having listened to the agencies and Canadians.

Welcome, Ms. Khalid. We're glad to have you and Ms. Petitpas Taylor as well. Thank you for joining us.

We're going to begin this round of seven-minute questions with Ms. Damoff.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, all, for coming. I would ask the chair to indulge me for just a moment.

Commissioner Paulson, when you appeared before, I certainly asked you about harassment in the RCMP. I just want to publicly thank you for your announcement this morning. It was historic. I'm very hopeful, as I know you are, that this will turn a page in a new chapter for the RCMP. Thank you for that.

Commissioner Bob Paulson (Commissioner, Royal Canadian Mounted Police): Thank you.

Ms. Pam Damoff: I also sit as vice-chair on the status of women committee. We heard recently from Carol Todd, whose daughter Amanda experienced cyber-violence from a predator in the Netherlands. That sort of ties in when we're talking about issues of cybersecurity.

Ms. Beauregard, when you appeared before the committee before, my colleague Mr. Spengemann asked you about a strategy to deal with these threats that are both domestic and international, because when we're dealing with the Internet, it's not a country; it's international. There were certainly challenges in that young lady's case in terms of dealing with the issues.

When you responded, you said that we didn't necessarily have a strategy in place. I'm wondering if you could elaborate on what we need to do, bearing in mind respect for the privacy of Canadians, particularly with regard to the international aspect. How can we best deal with that?

Ms. Monik Beauregard (Senior Assistant Deputy Minister, National and Cyber Security Branch, Department of Public Safety and Emergency Preparedness): Thank you very much for the question.

On the issue of cybercrime, cyber-bullying, and all that, as the minister pointed out, we currently have a consultation ongoing on the best ways to secure ourselves online. Specifically, the issue of cyber-bullying and cybercrime has manifested itself as a fairly significant preoccupation. Since then, before going online with the cyber review, we did modify it to include a fairly significant chapter that would address cyber-bullying, cybercrime, and all that.

● (1640)

Ms. Pam Damoff: It's not just with cyber-violence, though. I would suspect that even with issues of terrorism you'd be running into the same types of issues. We had a gentleman from the Association of Chiefs of Police who talked about how it takes 18 months to get evidence through signatories to the mutual legal assistance treaty. Do you run into that with terrorism threats as well?

Ms. Monik Beauregard: On that, GAC, Global Affairs Canada, is really the department that leads all the efforts with respect to international co-operation. What I was trying to get to was that as part of the cyber review, we are looking for feedback on how we can improve both domestically and internationally our measures to fight that.

You indicated that we don't have a strategy at this point. This is something we are looking forward to establishing with the end of the consultation. The consultation closes at the end of the month. By then we will have collected the feedback from all the stakeholders. As well, we've consulted with our international close allies on this issue. The results of all the consultation will be forwarded to cabinet.

Ms. Pam Damoff: Okay, thank you.

At our last meeting we heard a lot about metadata and how collection can impact privacy. I didn't have an opportunity to ask a question. I would suspect that most Canadians don't even know what metadata is. Can someone perhaps elaborate on how it's collected and how it does impact on our privacy?

Mr. Malcolm Brown (Deputy Minister, Department of Public Safety and Emergency Preparedness): Frankly, on the collection of metadata and the extent to which it's undertaken, I think you really need to turn to our colleagues at CSE. I don't think a huge amount of metadata is collected. I'll let my colleagues correct me, but generally speaking, it is essentially data that is the equivalent of non-personalized information about a device—the length of time, where that device is, and that kind of thing.

Perhaps my colleagues would like to take a stab at it.

Mr. Michel Coulombe (Director, Canadian Security Intelligence Service): I'll give you the example of email. Metadata would be everything except the content of the actual email. It would be the email address, the IP address. The phone number would be... although not in the case of the email. To go back to the old mail, it would be what you would find on the envelope, not the content of what's in that envelope.

My colleague from CSE would probably say that's a pretty crude description of metadata.

Ms. Pam Damoff: The Privacy Commissioner did express privacy concerns about the sharing of that data. You're saying it's similar to what's on an envelope.

Commr Bob Paulson: I would say that the Privacy Commissioner's concerns come from the raw collection of metadata from which certain trends or behaviours or conclusions about movements and so on can be deduced. We don't do that, and if we do do it, we do it through warrant, similar to our friends at the service. That's how we manage that.

Mr. Malcolm Brown: I'm not trying to pass the buck here, but I think if there are those kinds of questions about the theory around metadata, it would be more helpful if you had the experts from CSE to try to answer your question.

Ms. Pam Damoff: Thank you. I think that's my time.

Thank you for being here.

The Chair: That's very helpful, because as we looked at our witnesses, we had thought about CSE, then put them aside because they relate to other branches of government that we don't deal with. I suspect it would be helpful to now include them on our witness list, so thank you for that.

Mr. Miller.

● (1645)

Mr. Larry Miller: Witnesses, thanks very much for being here.

I want to start with you, Mr. Coulombe.

You appeared before a Senate committee on national security and defence. Afterwards, you issued a statement where you recognized some statistics regarding current intelligence on individuals. I believe that statement said that CSIS is aware of approximately 180 individuals who have travelled from Canada to participate in terror activities abroad. You're also aware of approximately 60 individuals—that has probably changed a bit—who have returned home from abroad. I have three questions on that.

Number one, why haven't these individuals been arrested? Two, are there ongoing investigations on those individuals? Three, what is the evidence threshold to detain them?

Mr. Michel Coulombe: Thank you for the questions, but two of the three questions are actually more law enforcement, so they would be for the commissioner.

In terms of the second question on ongoing investigations, I've also testified that—and I'm talking about the 60 returnees—it's important to understand that a returnee, somebody coming back from overseas who has participated in terrorist-related activities, poses a potential threat. They're not all the same. Some of them will come back and go back to a normal life. Some will continue to be engaged in threat-related activities.

We have ongoing investigations on some of them, but, again, it depends on the type of activities they've been involved in since they have come back.

Mr. Larry Miller: Would it be half of them who are under investigation? Do you have any numbers?

Mr. Michel Coulombe: Not off of the top of my head. I couldn't say how many of the 60 are—

Mr. Larry Miller: Sure, fair enough.

Mr. Paulson.

Commr Bob Paulson: We'll investigate anyone for whom we have a reasonable suspicion that there is a criminal offence being committed. The threshold for bringing charges, though, is a different question. We can arrest someone on reasonable grounds to believe, but we need the support of the prosecution service in order to (a) bring Attorney General consent to a terrorism charge, and (b) support a prosecution. There is an analysis that takes place, because if we were to arrest them we could only hold them for 24 hours, unless we made the case through the recognizance provisions of Bill C-51 that we could hold them for longer.

We try to build a case that will win in court. We enter into the discussion about the spectrum of activities that we collectively engage in to manage the threat, ranging from surveillance, to continued investigation interviews, to peace bonds, etc.

We have many, many active investigations, as do our colleagues at the service, and there's no one out there for whom we have evidence to bring a charge that we're not charging.

Mr. Larry Miller: Okay, I'm happy to hear that.

You mentioned the fact that you're only allowed to detain somebody for 24 hours. Has that changed with Bill C-51?

Commr Bob Paulson: Yes, it has. It brings with it new conditions that we would have to satisfy in order to extend past the 24 hours. We would have to appear before a judge and make the case that there is a need to detain the person past 24 hours as we collect evidence and so on.

The provisions for the continued detention come from the realization that the so-called "flash-to-bang time", in other words, when we learn about terrorists, and when they commit the act, has compressed over the years. I think that's everyone's experience internationally and certainly domestically. We realize that we might not have a presentable case in time, because it's very complex and logistically onerous to bring a case and persuade another human about the facts in a case.

Mr. Larry Miller: Okay.

Just carrying on, my next question is on whether it is now easier or more difficult to get a peace bond. Can you comment on that?

Commr Bob Paulson: It's supposed to be easier. That's not the answer to your question, though.

Mr. Larry Miller: Is that a good thing?

Commr Bob Paulson: It's supposed to be easier, but I think great care has to be taken with how.... I think it is a good thing. As I said once, in the right circumstances it's the only pre-charge control that the state can exercise over a suspect, short of a recognizance, or if there was a conviction, over a probation order, and so on. I think it's a good thing. I think that it's not well understood by Canadians. It's not well understood by a lot of people in terms of what it is. It certainly isn't a panacea, but it's a good thing.

● (1650)

Mr. Larry Miller: Louise Vincent, who is the sister of Warrant Officer Patrice Vincent who was killed, I believe in the Montreal area, appeared before the public safety committee. She stated that the RCMP had not been able to get a peace bond against Martin Couture-Rouleau due to a high evidence threshold. Has that changed? Is that true? Can you comment on that?

Commr Bob Paulson: Yes, I can. To be fair to everyone who was working on that case, on Couture-Rouleau, we had not.... We didn't obtain a peace bond on Couture-Rouleau. I think it's become easier since then to get a peace bond. Certainly the threshold has changed. Bill C-51 provides for a lesser threshold, which is "reasonable fear".

Mr. Larry Miller: I'm running out of time. There's a private member's bill before the House to define "variant", which is named 97 times in the Firearms Act. Would that bill be helpful to the RCMP?

Commr Bob Paulson: I don't know. I can't answer that. I'm not in a position to answer that.

Mr. Larry Miller: Okay. I have one last question. Going back to what we were discussing before that last question, would Warrant Officer Vincent, in your opinion, still be alive had Bill C-51 been in place?

Commr Bob Paulson: I don't think I can answer that, either.

Mr. Larry Miller: Okay. I have 12 seconds. The reason I asked that is a couple of people in law enforcement said as much. It might have been an opinion, but I just wanted to hear your answer on it. Thank you.

[*Translation*]

The Chair: We now move to Mr. Dubé.

Mr. Matthew Dubé: Thank you, Mr. Chair.

Ladies and gentlemen, thank you for joining us today.

Mr. Coulombe, I have in my hand a directive that the minister sent to your predecessor about sharing information, more specifically about what is described as mistreatment, but let's call it what it is, we are talking about torture. My colleague Ms. Laverdière and I have done a lot of work on this. One thing particularly concerns us, if you will allow me to quote the minister's letter.

> As a general rule, CSIS is directed to not knowingly rely upon information derived through mistreatment by foreign entities.

However, the letter continues as follows:

> In exceptional circumstances, CSIS may need to share the most complete information in its possession, including information from foreign entities that was likely to be derived through mistreatment...

Can you guarantee us that we are not currently using information obtained as the result of torture? I feel that Canadians would be of the opinion that it is unacceptable.

In addition, do you agree with us when we say that this is the kind of directive that we should discontinue? You have to make sure we are protected, but we also want our values protected. In our opinion, this does not correspond to our values at all.

Mr. Michel Coulombe: Actually, in the annual report that was recently tabled by the Security Intelligence Review Committee, SIRC, the matter of exchanging information with foreign partners was studied.

SIRC found that, after that departmental directive, the Canadian Security Intelligence Service, CSIS, quickly established governance policies to make sure that it is complying with its legal obligations and following the minister's directive.

That includes a high-level committee that meets to assess the risks involved in mistreatment or torture. If ever we exchange information, the committee must evaluate how it may have been obtained and must decide whether we should use it or not. If that assessment carries a high risk, I am the person who has to make the final decision to share or to use the information we have received.

SIRC says that CSIS has established a very rigorous structure in order to meet its obligations as to mistreatment as well as its obligation to protect Canadians, which is its primary mandate.

To answer your second question quickly, I will say that it is a policy matter that is up to the government and to Parliament to debate and decide.

Mr. Matthew Dubé: Okay.

In terms of the discretionary aspect, information obtained as a result of torture is considered to be almost 100% ineffective. So it cannot really be said that Canadians' security is assured.

Is it really necessary to use information obtained as a result of torture?

● (1655)

Mr. Michel Coulombe: It is said that information obtained as the result of mistreatment is often untrustworthy, and I am not here to try to contradict that. The fact is that, if we have information obtained as the result of torture, we are aware that the information may not be trustworthy and we try to find other sources in order to corroborate it. We must also decide if we are going to keep that information to ourselves, even in cases where police forces could act to prevent an incident that is about to happen.

We are aware of that and we take it into account in the measures we undertake. Either we try to find other sources to corroborate the information or we determine the use we will make of it, knowing that it is doubtful that the information can be trusted.

It would be irresponsible for CSIS to simply dismiss the information out of hand if there is a clear and present danger to Canadians.

Mr. Matthew Dubé: Speaking of sharing information between consular services and Global Affairs Canada, pursuant to the provisions of Bill C-51, how can we be sure that we will not run into another case like that of Maher Arar, where information obtained as a result of torture did not seem to be discredited?

Bill C-51 also provides for agreements that allow information on Canadians detained abroad to be obtained.

In circumstances like those, how can we assure Canadians that the information that you are sharing has not been obtained as a result of torture and we are not once more going through that experience that was supposed to be an opportunity for learning and major reform?

Mr. Michel Coulombe: Today, we have legislation that deals with the exchange of information in the particular case you mentioned, that is between Global Affairs Canada and the service. That did not exist three years ago or even last year. As has been announced in the media, CSIS and Global Affairs Canada have recently signed a protocol. Before that—

Mr. Matthew Dubé: I am sorry to interrupt you, but my time is limited.

What exactly are the specific protections provided for in the legislation that would prevent such a situation from happening?

Mr. Michel Coulombe: It is the Security of Canada Information Sharing Act, which comes about as the result of Bill C-51. It must be said that the act is not binding on other departments.

Mr. Matthew Dubé: Nevertheless, an agreement exists.

Mr. Michel Coulombe: The use of the act remains voluntary. It is to facilitate the exchange of information.

As for protection, the act stipulates that the agency providing the information must make sure that the information is relevant to the recipient institution's jurisdiction.

Mr. Matthew Dubé: Let's keep going with that logic.

[*English*]

I have a copy in English here in front of me. If we talk about the threshold that exists, relevant versus necessary—I think that's what we've got into—the Privacy Commissioner said that that threshold should be changed. Basically, the situation we're now in is that information is subject to a lower threshold, so there really isn't a very large legal protection to avoid a similar situation like we've seen in the past.

Mr. Michel Coulombe: I'm not in a position to debate legal threshold, but the other protection we haven't talked about, and I've just mentioned it, is the fact that the Privacy Commissioner can review the information that was exchanged. In the case of the service, SIRC can review all the information that we receive through what is known as SCISA, the act that came through Bill C-51. I believe there is protection.

Now, should the threshold be higher or lower? Again, that's a policy decision for parliamentarians and the government.

[*Translation*]

Mr. Matthew Dubé: Thank you.

[*English*]

The Chair: Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: I want to start with a quick question for Mr. Coulombe on disruption powers. Perhaps you could give the committee an update on the number of times the new threat reduction powers have been used.

Mr. Michel Coulombe: I think it was February that I was in front of this committee. At the time I believe I mentioned something around two dozen, if I'm correct. My answer will still be the same because we're not doing a huge number of them. It could have been 18 at the time, and now it's 20.

● (1700)

Mr. Nathaniel Erskine-Smith: It might be 20?

Mr. Michel Coulombe: Yes, it might be 20. An important point to specify is that all of them didn't require Federal Court warrants.

Mr. Nathaniel Erskine-Smith: That's understood, because you weren't seeking to deal with the charter anyway, and we heard that from the minister.

With respect to these disruption powers, I want to get at the heart of this. Can you speak to why these powers are necessary, and perhaps give us specific examples of where the pre-Bill C-51 powers were insufficient and why existing law enforcement powers are insufficient.

Mr. Michel Coulombe: When it comes to our mandate, our threshold to investigate is lower. We're in the position at the very emergence of a threat to be there and to see the evolution. As the commissioner just mentioned, that evolution today from planning to execution, and from radicalization to mobilizing to use violence, means that time is extremely short. Threat reduction can be useful in scenarios where we want to reduce that threat as soon as possible, and that's something we couldn't do before.

Mr. Nathaniel Erskine-Smith: What I'm trying to get at is that "threat reduction" is a very broad term. I know that in other countries they specify the powers in a less vague way, to put it politely. Specifically, what are examples for Canadians to know? When we say "threat disruption" or "threat reduction", what are we talking about?

Mr. Michel Coulombe: There are examples in the green paper. I think when I testified previously, I gave an example that "non-warranted" can be as simple as asking somebody to intervene because a young person is on the path to radicalization and mobilizing to violence. It could be informing the parents that their kid is on that path. It could be advising social media that a user is breaching their rules. The service will not take down the account, and it's up to the social media to do it. Those simple things we couldn't do before.

Mr. Nathaniel Erskine-Smith: If we go back to 1981, the McDonald Commission found that security intelligence should be separated by police work. Could you speak to One Vision 2.0 and give a quick explanation of that to the committee? Could you speak to whether we should codify One Vision 2.0 and the requirement for collaboration and notification between the RCMP and CSIS?

Mr. Michel Coulombe: Sorry, if...?

Mr. Nathaniel Erskine-Smith: Perhaps you could comment as to whether that should be long-standing and we should codify that.

Mr. Michel Coulombe: You mean the relationship...?

Mr. Nathaniel Erskine-Smith: Give a brief explanation of One Vision 2.0. Is it working? Is it something we should—

Mr. Michel Coulombe: Oh, it's a framework. It's a framework for CSIS personnel and the RCMP when we're looking at the same investigation and how to do this. To make sure there's notification and no gaps is extremely important for us, and that whatever we're going to be doing will not have a negative impact on the criminal investigation further down the road for a criminal prosecution.

Mr. Nathaniel Erskine-Smith: You're not having two separate parallel tracks, but you're in communication.

Mr. Michel Coulombe: Exactly.

Mr. Nathaniel Erskine-Smith: Okay.

Moving to Commissioner Paulson, with preventive arrest and the expansion of preventive arrest, you mentioned a lowering of the threshold. Is that lowering of the threshold necessary? Has this preventive arrest power been used since Bill C-51?

Commr Bob Paulson: No, it has not been used. I would continue to argue that it's nice to have, given how we understand the threat because of what I described and what my colleague described, as well. The difficulties we have in getting the information, as complex as it is, unpacked as it often needs to be, and presented coherently to a prosecutor to be able to make all the decisions takes a lot of time. That's the advantage, in my mind.

Mr. Nathaniel Erskine-Smith: Since it hasn't been used, then is it fair to say we don't have any evidence that lowering the threshold is necessary or that the increase from three to seven days was necessary?

Commr Bob Paulson: We don't have any evidence different from what we had to have a change in the first place.

Mr. Nathaniel Erskine-Smith: Okay.

I'd asked the minister about a super-SIRC and a larger review body. I'm curious you would have no position on this. I mean, obviously there is a review body already that governs CSIS and that governs the RCMP. Would you be supportive of a super-SIRC that could share information and match whole-of-government security with whole-of-government review? Would you have no issue with it?

Commr Bob Paulson: I don't take any issue with any oversight. I think the need to coordinate the oversight—because there is no shortage of oversight in my mind—and to have it coherent is important.

● (1705)

Mr. Nathaniel Erskine-Smith: Yes, so the existing review bodies would coordinate together and perhaps we would pull the CBSA into the review, as well.

Mr. Coulombe, would you have any thoughts on that?

Mr. Michel Coulombe: That's a policy issue to be decided by government, and the service will, whatever tools are put in place, review and have oversight over the service, and—

Mr. Nathaniel Erskine-Smith: There's no issue with that.

Mr. Michel Coulombe: —we'll co-operate and work within that framework.

Mr. Nathaniel Erskine-Smith: Perfect.

There's a definition in the SCISA, "activity that undermines the security of Canada", and it's a very different definition from that in the CSIS Act, "threats to the security of Canada".

Mr. Coulombe, would you have any issue if we stuck with the "threats to the security of Canada" definition in the CSIS Act? That's the one you've always operated under.

Mr. Michel Coulombe: I'll talk about the CSIS Act. We continue.... SCISA didn't change anything.

Mr. Nathaniel Erskine-Smith: It changed the definition.

Mr. Michel Coulombe: Well, not for us. We still work under the CSIS Act, so for what we do, the definitions are in section 2 of the CSIS Act.

Mr. Nathaniel Erskine-Smith: Where information is shared, though. I should specify where information is shared is now subject to SCISA, which is a broader definition. My point is, if we talk about information sharing, would you have any concerns with information sharing being limited to "threats to the security of Canada", the definition in the CSIS Act?

Mr. Malcolm Brown: Let me take a stab at this because we have to be careful about "would we have any concerns". There is the old maxim that silence deems consent. We have to be careful about that.

We have to remember that SCISA covers more than the service. It covers 17 departments and agencies, many of which don't have any definition at all. I think the rationale for the definitions in place is, in fact, to provide guidance to other departments and agencies that are operating in a completely different context from the service.

Mr. Nathaniel Erskine-Smith: I'm out of time. Would you follow up in writing if you have specific concerns with the difference in definition and if the sharing of information was actually limited to "threats to the security of Canada" as defined in the CSIS Act?

The Chair: Thank you.

[*Translation*]

Mr. Généreux, you have seven minutes.

Mr. Bernard Généreux: Thank you, Mr. Chair.

Thank you to the witnesses.

Mr. Coulombe, the government assures us that, when it comes to immigration and the processing of refugees, CSIS conducts security checks on potential newcomers to Canada. Is that correct?

Mr. Michel Coulombe: We are responsible for the national security component, but there are other aspects.

Mr. Bernard Généreux: The RCMP handles those, does it not?

Commr Bob Paulson: Sorry, I didn't understand your question.

Mr. Bernard Généreux: The government has told us that, when it comes to immigration and the processing of refugees, security checks are conducted. Mr. Coulombe said that his service did a portion of that work, and I imagine the RCMP does the other portion. Is that correct?

Commr Bob Paulson: Yes, we have a role in the security checks carried out.

Mr. Bernard Généreux: In your role, do you go as far as checking social media? Which technology platforms can you look at without violating people's privacy? What's the balance there?

[*English*]

Commr Bob Paulson: For us, we do a series of things. On immigration files, we will do our police holdings, but it's quite clear that, if people are seeking to come to this country, it's very unlikely that they have much of a history in this country in terms of the traditional criminal indices checks, but we do our indices checks. We check fingerprints. We check other things. We check open-source material. The intrusion on privacy isn't a huge consideration, given that we're doing these indices checks that are governed according to existing statutes.

[*Translation*]

Mr. Bernard Généreux: Following the events that occurred in San Bernardino, California, U.S. homeland security officers told ABC that they weren't permitted to check social networks for information on people because of privacy laws.

Is that the same in Canada?

[*English*]

Commr Bob Paulson: It's not my experience.

Mr. Bernard Généreux: You're allowed, then. You can use social media.

Commr Bob Paulson: Yes, we do. Not to overstate it, but we do what we refer to as open-source checks. We'll check the Internet for available information, which will give us some indication, like we do for applicants to the RCMP and for security clearances in support of the broader government efforts to understand who we're dealing with.

● (1710)

[*Translation*]

Mr. Bernard Généreux: Social networks don't pose a privacy issue, then.

[*English*]

What's the line there?

Commr Bob Paulson: I don't know that there is a clear line. For people who use social media, we don't do any sort of search and seizure. We're looking at records that are in the public domain; therefore, if we find that we have to do some searching, like a traditional search pursuant to how searches are generally understood, we would get a search warrant. But it's Facebook, Google, and those kinds of things.

[*Translation*]

Mr. Bernard Généreux: Has the passage of Bill C-51 had an impact on the tools in your arsenal to conduct more in-depth investigations of certain individuals, either giving you more such tools or enhancing them?

[*English*]

Commr Bob Paulson: No, not really. It didn't have any impact.

[*Translation*]

Mr. Bernard Généreux: As part of the committee's study, we have to consider the technology side of things. We talked about it earlier. The minister indicated that, in the technological realm, some threats were detectable in certain cases, but same but not in others. He mentioned the "going dark" phenomenon, where activities fall completely under the radar and therefore can't be detected. For that matter, I don't even know how he knows about them, since they are under the radar, but I imagine you have tools that tell you they're out there.

Can you discuss the potential technological threats that hackers or various groups could use to target Canada or Canadians?

Commr Bob Paulson: Thank you for the question.

I'll start the answer off, and then my colleague can round it out.

[*English*]

This is the single most important issue that we have, certainly from the police, and I know that I speak for my colleague when we talk about how we're going forward to deal with encryption, and going dark, and managing things on the Internet. It is, as I said, the single greatest impediment to our effective investigations as we proceed with managing the terrorist threat.

The Chair: I'm afraid I need to end it there.

Mr. Mendicino.

Mr. Marco Mendicino: Witnesses, thank you for attending today and for your testimony.

I want to draw your attention to what is now section 12.1 of the CSIS Act. It's a section that has attracted a lot of public dialogue and, to be fair, a lot of criticism, to put it bluntly. The section essentially authorizes the service to undertake certain measures that could potentially infringe on the charter.

I want to verify that the provision has not been used to date.

Mr. Michel Coulombe: That's correct.

Mr. Marco Mendicino: Was the service consulted by the last administration of the need for this particular provision?

Mr. Michel Coulombe: Yes.

Mr. Marco Mendicino: Are you at liberty to say whether the service's position was that this provision was needed in order for you to fulfill your mandate?

Mr. Malcolm Brown: There is a convention that advice to a previous government stays with the previous government, and most governments like it, particularly when they are no longer the government, which happens from time to time.

I would encourage my colleague to—

Mr. Marco Mendicino: —abide by that convention?

Mr. Malcolm Brown: —restrain himself.

Mr. Marco Mendicino: Okay.

The reason I'm asking the question is that, as part of this consultation, I anticipate that we will hear from a number of witnesses who will say that the section 12.1 provision that would authorize service personnel from undertaking threat reduction activities which could infringe their charter rights is not necessary for the purposes of CSIS fulfilling its mandate.

In the spirit of anticipating those questions, I wonder whether you might comment about whether there might be improvements made to that particular section in a way that is respectful of the charter.

[*Translation*]

Mr. Michel Coulombe: Of course, it can't infringe upon the charter.

[*English*]

I've just said that we've used the threat reduction measures about two dozen times now, so I cannot sit here and say that it's not useful. We've used it.

What I can say, though, is that the way that new mandate is articulated in our act could be looked at, could be changed, or could be left as it is. Again, that's a policy decision, and that's not for me to decide. The service will work with the tools it's provided with, but the tool itself, in the current threat environment, I believe is useful.

● (1715)

Mr. Marco Mendicino: Can I put it to you another way?

Prior to the introduction of what is now section 12.1 of the CSIS Act, was there a prevailing view that CSIS was not able to fulfill its mandate?

Mr. Michel Coulombe: Well, it depends on what you talk about as mandate. We were able to fulfill our previous mandate, which was to investigate and advise government. What we couldn't do was reduce the threat. Threat reduction didn't have any impact on the mandate we had until Bill C-51, which was to advise government.

What was felt...and in fact if you go back to 2010, SIRC raised this issue. The whole issue of the service not being able to disrupt a threat was raised at a special Senate committee on terrorism. It had no impact on our previous mandate to advise government, but it had an impact in terms of being able to reduce the threat in the current environment, where it's fast paced, there is much more volume, technology, encryption, and we just talked about going dark. Therefore, it's an additional tool that we can use.

Mr. Marco Mendicino: I should be a little bit more specific. What I'm referring to are those threat reduction activities that could potentially infringe the charter. If you look at that in the two subcategories, I'm really referring to the latter. I am looking at those activities which, under subsection 12.1(3), could infringe the charter. Do you have any views about that today that you're able to share?

Mr. Malcolm Brown: Well, Michel may want to add a bit. The minister and Michel have both said that it's never been used. I think the question is difficult for officials to respond to. There are scenarios that could be described, and the green paper—

Mr. Marco Mendicino: I'm sorry, but I'm going to have to interrupt because I want to get one last question in before I lose my time.

Do you take anything from the absence of having to use those powers since the last time we asked? Is there a trend developing that perhaps you don't need them as much as you did the last time you reported, or is it just happenstance?

Mr. Michel Coulombe: No, the fact that we haven't used them doesn't mean that we couldn't use them.

Mr. Marco Mendicino: I understand. Thank you.

The Chair: Mr. Brassard.

Mr. John Brassard: Thank you all for being here today.

Commissioner Paulson, I want to pick up on something you ended on with Mr. Généreux, and the single most important issue that you face with respect to managing threats, encryption, and going dark. The green paper speaks to lawful access in the absence of a clear law governing access to basic subscriber information—name, address, IP, for example. It has made it difficult for law enforcement to obtain it in a timely and effective manner.

Some other countries allow police and intelligence agencies to obtain basic subscriber information without going to court. In your opinion, should we be looking at amending the legislation to allow law enforcement and intelligence agencies to obtain basic subscriber information without a warrant? I'd like to hear from all three of you on whether there are any other changes within the scope of this national security framework that we're looking at that law enforcement or cyber would like to see changed or amended.

Commr Bob Paulson: I'll start and say absolutely, yes. I have advocated publicly and aggressively for basic subscriber information without warrant, to my peril in many instances, but I think it's vital. I think the encryption discussion has not yet fully taken place, and the understanding of the implications for privacy concerns is not well distributed. In other words, people don't have a fair understanding of what we're talking about.

To use my colleague from the FBI's analogy, it used to be that the corner of the room was dark and we were all happy with that because we knew that, say, foreign governments or espionage networks were working in this very clandestine place where we couldn't see. But that darkness has crossed into the lion's share of the room now. Traditional criminality, like terrorism, organized crime, child exploitation, and fraud, is being advanced, supported, and accelerated by the availability of these commercial encryption programs.

It's devastating to counterterrorism investigations, and it's a big challenge.

● (1720)

Mr. John Brassard: Mr. Coulombe, do you have anything you'd like to add to that?

Mr. Michel Coulombe: The only thing I'll add is that it's important to understand that the "going dark" issue is broader than subscriber information and encryption. It's that, but it's also intercept-capable networks, and datasets sitting in a foreign country that we don't have access to but that are used by Canadians. It is important to understand that "going dark" is a complex issue. It's multifaceted, and it needs to be understood.

I totally agree that it has a huge impact on our investigations. Some of our targets encrypt the vast majority of their communications.

Mr. John Brassard: With respect to information sharing between not just domestic agencies but foreign agencies as well, are there improvements that need to be made in that regard that we should be looking at from a legislative standpoint?

Commr Bob Paulson: Well, my colleague from Public Safety addressed one of the government questions about MLATs, and so on. It's a cumbersome process. It's very legalistic. It takes a lot of time. We have to do better there, frankly. I've raised that with my colleagues at Justice. It is, by its nature, cumbersome, so we need to think it through. Never mind the assessments of the practices of the foreign country with respect to your other colleagues' questions, just the legal process of getting the evidence into Canada so we can use it in court is very cumbersome.

Mr. John Brassard: The green paper also speaks of threat reductions, but in it there is no distinction between home and abroad. How would you classify that distinction?

Mr. Coulombe, obviously that question would go to you.

Mr. Michel Coulombe: There is no distinction. We can actually fulfill our mandate, both investigate the device and threat reduction, here and abroad. Internally, the same policy applies. It's all based on risk evaluation. The risk might be higher if it is outside the country, but in terms of the management of those operations, there is no distinction.

Mr. John Brassard: Thank you.

The Chair: Thank you very much.

Monsieur Di Iorio, go ahead.

[*Translation*]

Mr. Nicola Di Iorio: Thank you, Mr. Chair.

Thank you again for being with us today.

I'd like to talk to you about the radicalization phenomenon and the role of communities. It's clear that radicalization has an impact on families whose children take part in violent activities. Those families belong to a community. How can those communities prevent, detect, and combat radicalization? What role do you think they can play?

I'll give you some context. You manage large groups of people. But, surely, people who belong to the communities either directly or indirectly affected by radicalization can, on a volunteer basis or what have you, lend some support to the efforts of law enforcement officials.

Mr. Michel Coulombe: They play a crucial role on a number of levels. Having people who have observed signs of radicalization share that information with CSIS or police forces like the RCMP is key. That's an extremely important network for us.

The best example of that is the initiative that was put in place in Montreal to help communities and families prevent radicalization. CSIS intervenes as soon as the radicalization process is triggered and the radicalized individual poses a threat. Communities and families play a vital role from a prevention standpoint. I think Montreal's initiative is a great model.

● (1725)

Mr. Nicola Di Iorio: What are you referring to?

Mr. Michel Coulombe: The Centre for the Prevention of Radicalization Leading to Violence.

Mr. Nicola Di Iorio: The centre, though, is funded and employs people to do that job. That's not what I mean. I mean people from the community who take it upon themselves to intervene and support the efforts of law enforcement agencies, such as yours and Mr. Paulson's, without being paid to do so.

Mr. Michel Coulombe: It's all of that combined.

Ms. Beauregard could elaborate on that.

Ms. Monik Beauregard: I completely agree with the director of CSIS. It's absolutely crucial to work with as many stakeholders as possible, be they the communities, themselves, social partners, law enforcement, the provinces and territories, or the municipalities. It's a collective effort all over the country.

Mr. Nicola Di Iorio: My apologies, but I have to stop you there. I understand the collective effort principle, but I want to get back to my point. I don't want to talk about structured groups or organizations that receive public funding, like the centre in Montreal. I want to talk about the potential role of people who are directly affected by radicalization or whose loved ones or communities are affected.

My question is for Commissioner Paulson, who, I believe, has members on his staff involved in community outreach.

[*English*]

Commr Bob Paulson: First of all, let me just endorse what the government is doing with respect to the coordination of counter-radicalization work and public safety.

As you know, the police experience, outside of counterterrorism, has been to engage with the very people you are talking about, to have crime prevention strategies, to have outreach initiatives, to inform the citizens of a given community about the risks of criminality and about prevention. We are using that, through the CACP, the RCMP, and other mechanisms, to take advantage of those outreach connections into communities to inform citizens and to alert them, particularly those who are at risk, to what they can look for and what resources are available to support them in their problems. So I agree.

Mr. Nicola Di Iorio: Are there powers you don't currently have that you deem you would need?

Commr Bob Paulson: I think it's a very delicate area that has to be trod upon very carefully, particularly by the police, as we go into.... I talked to the FBI recently about their counter-radicalization efforts. They're very circumspect about wanting to take on the responsibility of counter-radicalization. I assert the police potential for using these pre-existing networks into communities, because in Canada, crime prevention is how we do community policing.

Mr. Malcolm Brown: I think there's lots of evidence that demonstrates grassroots, community-based efforts on counter-radicalization are the most effective. One of the challenges is not to design a "we're from Ottawa and we're here to help" program across the country in terms of counter-radicalization, but to build on best practices to share that the vast majority of it is grassroots, led by family members who have gone through the experiences you've just described. I think we're pushing on an open door here.

The challenge is also to recognize that counter-radicalization has limits. You have to do it. It does pay dividends, but it's not going to prevent every threat that we're going to otherwise confront.

The Chair: Thank you, Mr. Brown.

[*Translation*]

I think that, for the first time, Mr. Dubé will have the last three minutes of speaking time.

Mr. Matthew Dubé: Thank you.

I'd like to keep talking with Mr. Paulson.

I have a question about the stories that have come out in recent years regarding the RCMP's use of resources. According to those stories, the resources allocated to counterterrorism efforts meant that the force lacked the resources necessary to deal with other issues such as organized crime. Is that still the case?

This is an area where we talk a lot about legislation. Sometimes, though, the solutions are much simpler than that. Could we not just give the men and women whose job it is to keep our country safe the resources they need?

[*English*]

Commr Bob Paulson: I agree. We are looking at our resourcing levels. We continue to transfer people out of other areas into counterterrorism investigations. Our officers are underpaid in comparison to their counterparts in city police forces. It's a very difficult HR environment to continue to maintain the pace of operations that we have.

● (1730)

Mr. Matthew Dubé: That's good to hear. When the debate goes on about what could or could not be done in cases that are tragically behind us, I'm wondering about the weight of legislation versus resources, because I believe, as many others do, that sometimes the solution is not necessarily changing the laws, as was done under the previous government, but ensuring that police have the resources to be able to enforce existing laws.

Would you agree with that? Perhaps you could elaborate on what your experience has been.

Commr Bob Paulson: I would agree. My colleague at the service would agree with that. My colleague and I are running hard in the counterterrorism business, and you have to wonder at what point it's not just a temporary transfer of resources. I think I've said in the past, and I know Michel has, that it's not sustainable for the long term. We are meeting the threat, and we are managing as best we can, but there are costs for that.

As to the balance between legislation and resources, I think that's for you to decide after you've seen all the evidence.

[*Translation*]

Mr. Matthew Dubé: I have one last question.

Can you tell us which areas the RCMP has abandoned in order to focus its efforts on the fight against terrorism? What is currently being sacrificed because of the resource shortage?

[*English*]

Commr Bob Paulson: Abandon is perhaps a little too strong a word, but we've taken our investigative resources from areas of organized crime and financial integrity work. Our federal policing mandate, which is manifold, is predominantly focused on the counterterrorism threat.

[*Translation*]

Mr. Matthew Dubé: Thank you.

[*English*]

The Chair: Thank you again for coming to our committee meeting, and no doubt we will see you again over the course of this year.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca

3103(93/01)

Follow-Up Response
Appearance of the Minister and Senior Portfolio Officials before the Standing Committee on Public Safety and National Security Regarding Framework (Green Paper Consultations)
Thursday, October 6, 2016

Mr. Nathaniel Erskine-Smith: There's a definition in the SCISA, activity that undermines the security of Canada, and it's a very different definition from that in the CSIS Act, threats to the security of Canada. Mr. Coulombe, you'd have no issue if we stuck with the threats to the security of Canada definition in the CSIS Act? That's the one you've always operated under.

Mr. Michel Coulombe: I'll talk about the CSIS Act. SCISA didn't change anything.

Mr. Nathaniel Erskine-Smith: It changed the definition.

Mr. Michel Coulombe: Well, not for us. We still work under the *CSIS Act*, so for what we do, the definitions are in section 2 of the *CSIS Act*.

Mr. Nathaniel Erskine-Smith: It's where information is shared, though. I should specify where information is shared is now subject to SCISA which is a broader definition, my point being if we talk about information sharing, would you have any concerns with information sharing being limited to threats to the security of Canada, the definition in the *CSIS Act*?

Mr. Malcolm Brown: Let me take a stab at this because we have to be careful about "Would we have any concerns". There is the old maxim that silence deems consent. We have to be careful about that. We have to remember SCISA covers more than the service. It covers 17 departments and agencies, many of which don't have any definition at all. I think the rationale for the definitions in place is in fact to provide guidance to other departments and agencies that are operating in a completely different context from the service.

Mr. Nathaniel Erskine-Smith: I'm out of time. Would you follow up in writing if you do have specific concerns with the difference in definition and if the sharing of information was actually limited to threats to the security of Canada as defined in the *CSIS Act*.

RESPONSE

An "activity that undermines the security of Canada" is defined in section 2 of the SCISA as any activity that undermines the sovereignty, security or territorial integrity of Canada or the lives or security of the people of Canada.

This definition is intended to facilitate the sharing of information relevant to the different national security mandates and jurisdictions of Government institutions. CSIS is only one of these institutions; other departments and agencies operate under different legislation and with different mandates. As a result, the definition in the SCISA is broader than "threats to the security of Canada" as found in the *CSIS Act*.

The SCISA does not affect recipient institutions' collection authorities. In the case of CSIS, any disclosed information needs to meet the requirements of the *CSIS Act* before it may be collected.

Under the SCISA, institutions should not send anything that is outside the recipients relevant jurisdiction or responsibilities. To prevent such an occurrence, institutions are encouraged to engage in a dialogue before disclosing information under the SCISA. For example, if CSIS were to receive information from another department or agency that meets the SCISA definition of "activity that undermines the security of Canada" but that does not meet the more narrow *CSIS Act* definition of "threats to the security of Canada" as per section 12 of the CSIS Act then CSIS would not collect or retain that information..

Follow-Up Response
Appearance of the Minister and Senior Portfolio Officials Before the Standing Committee on Public Safety and National Security Regarding the National Security Framework (Green Paper Consultations)
Thursday, October 6, 2016

Threat Reduction Activities

CSIS has issued under two dozen approvals for threat diminishment measures since the mandate came into effect in June 2015. None have required a warrant.

Examples of Non-Warranted Threat Reduction Activities

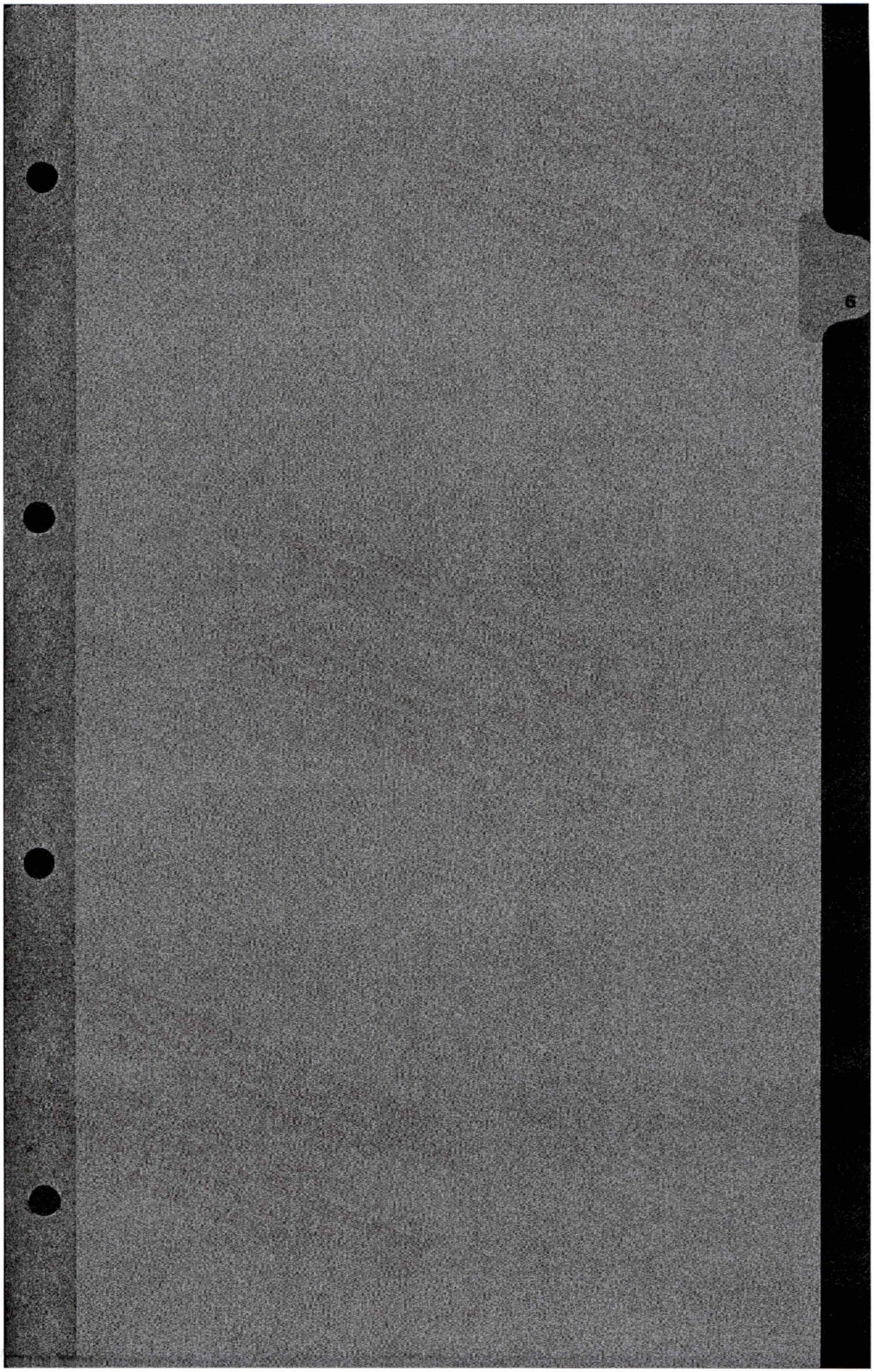
It is possible to generally describe examples of non-warranted Threat Reduction Activities but caution must be exercised as each measure would be assessed on its own merits to determine the authorization required. Non-warranted Threat Reduction Activities could potentially include:

- Employing human sources to provide a cautionary voice or counter-narrative;
- Asking a trusted associate of a prospective terrorist traveller, such as a family member, to intervene to dissuade the person from travelling;
- Making a person aware of CSIS' investigation through interviews with the person, family members or associates in order to dissuade the person from taking certain actions;
- Providing online counter-narratives;
- Calling a hostile foreign intelligence operative in for an interview, or informing the contacts of a known hostile foreign intelligence officer that their affiliation is known to authorities; and,
- Reporting social media accounts for violation of terms of use (hate speech/graphic violence).

Examples of Warranted Threat Reduction Measures

It is also possible to generally describe examples of TRA requiring judicial authorization, however, caution must be exercised as each measure would be assessed on its own merits to determine the authorization required. Warranted Threat Reduction Measures could potentially include:

- Intercepting and/or degrading equipment or weapons destined for terrorist or weapons-of-mass-destruction purposes;
- Modifying or removing threat-related content on an extremist website; and,
- Disabling or altering personal electronics (computer, phone) used to support threat activities.


6

House of Commons Standing Committee on Public Safety and National Security (SECU)

GOVERNMENT MEMBERS

Liberal Party of Canada

Robert Oliphant
(Don Valley West, Ontario)
CHAIR
- MP From 2008 – 2011
- Returning MP in 2015
- Former member of SECU (Jan – Dec 2009)

Pam Damoff
(Oakville North - Burlington, Ontario)
- First-Time MP
- Member of FEWO

Nicola Di Iorio
(Saint-Léonard — Saint-Michel, Quebec)
- First-Time MP
- Member of REGS

René Arseneault
(Madawaska – Restigouche, NB)
- First-Time MP
- Attorney specializing in corporate law and civil litigation

Michel Picard
(Montarville, Quebec)
- First-Time MP
- Former Parliamentary Secretary to Minister of Public Safety

Sven Spengemann
(Mississauga – Lakeshore, Ontario)
- First-Time MP
- Served as a senior United Nations official in Iraq
- Member of NDDN

OPPOSITION MEMBERS

Conservative Party of Canada

Larry Miller
(Bruce-Grey-Owen Sound, Ontario)
FIRST VICE-CHAIR
- MP Since 2004
- **Deputy Public Safety and Emergency Preparedness Critic**

Tony Clement
(Parry Sound-Muskoka, Ontario)
- Former President of the Treasury Board
- **Public Safety Critic**

Dianne L. Watts
(South Surrey-White Rock, BC)
- First-Time MP
- **Infrastructure and Communities Critic**
- **Urban Affairs Critic**

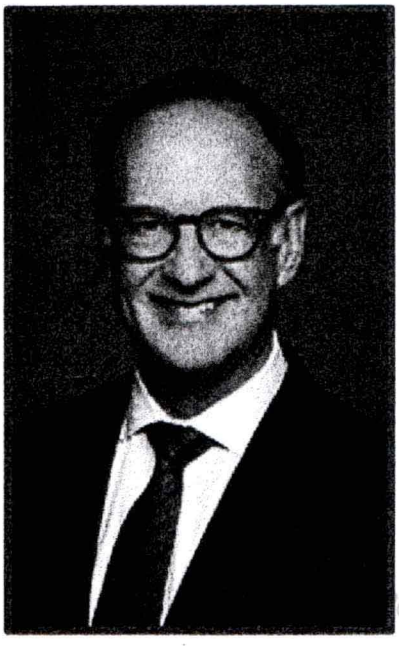
NDP

Matthew Dubé
(Beloeil — Chambly, Quebec)
SECOND VICE CHAIR
- Deputy NDP House Leader
- MP Since 2011
- **Public Safety Critic**
- **Infrastructure and Communities Critic**

RDIMS #1745867

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada



CHAIR

Name: **Robert Oliphant**
Riding: **Don Valley West, Ontario**

Parliamentary Experience:

- MP From 2008 – 2011
- Returning MP in 2015

Activities/Experience of Interest to the Portfolio:

- Former Member of SECU (Jan – Dec 2009)
- Provided chaplaincy services at Whitehorse Correctional Centre (Commissioner Head was Warden)

Rob Oliphant is the former President and CEO of the Asthma Society of Canada, a national health charity and patient organization. He is a community leader with a long history of advocating for poverty reduction, affordable housing, at-risk youth, and seniors' economic security. Much of this advocacy has been through his work as an Ordained Minister of the United Church of Canada. He served as a Senior Minister at Eglinton St. George's United Church in Toronto for ten years.

Rob Oliphant is a founding member of Affirm Canada, an organization that has advocated on behalf of members of the LGBTTQ community since 1982. He was also the founding chairperson of Neighbourhood Interfaith Group, which seeks to promote Christian-Jewish-Muslim dialogue.

From 2008 to 2011, Rob Oliphant was the Member of Parliament for Don Valley West, and served as the Opposition Critic for Veterans Affairs and Multiculturalism. Mr. Oliphant worked as a senior advisor in the Ontario government of Premier David Peterson in 1989, and was the Chief of Staff for two Ontario Ministers, Mavis Wilson and Christina Hart. Rob Oliphant was also the Chair of the Special Joint Committee on Physician-Assisted Dying. He is currently a member of the Liaison Committee (LIAI).

He holds a Bachelor of Commerce from the University of Toronto, a Master of Divinity from the Vancouver School of Theology at the University of British Columbia, and a Doctor of Ministry from the Chicago Theological Seminary at the University of Chicago.

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada

Name: **René Arseneault**
Riding: **Madawaska – Restigouche, NB**

Parliamentary Experience:

- First-Time MP

Activities/Experience of Interest to the Portfolio:

- Attorney specializing in corporate law and civil litigation

René Arseneault is a lawyer specializing in corporate law and civil litigation for more than 20 years, in which Mr. Arseneault established his own practice in 1996 with his spouse. He is also a singer-songwriter who in 1989 won the Prix du public [people's choice award] at the Gala de la chanson de Caraquet.

In addition to providing pro bono legal services, Mr. Arseneault has sat on the board of directors for numerous non-profit organizations. He co-founded the Balmoral Economic Development Association, Fondation École Régionale BDES inc. and Coopérative Radio Restigouche ltée – which he currently serves as Chair of the Board of Directors. René has also been involved in youth sports development, specifically as a soccer and volleyball coach and assistant coach, and as a volunteer at the Jeux de l'Acadie.

René holds a BSocSc – with a major in Economics and a minor in Political Science – and an LLB from Université de Moncton.

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada

Name: **Sven Spengemann**
Riding: **Mississauga – Lakeshore, Ontario**

Parliamentary Experience:

- First-Time MP
- Current member of NDDN

Activities/Experience of Interest to the Portfolio:

- Served as a senior United Nations official in Iraq
- Worked for PCO

Sven Spengemann was born in Berlin, Germany, and moved to Canada with his family at age 14. He volunteers at the Compass Food Bank and serves on the Board of Directors of United Way of Peel Region and the UTM Alumni Association. Mr. Spengemann is also an Advisor to the Peel Multicultural Council.

Mr. Spengemann's academic qualifications include degrees from the University of Toronto (Mississauga), Osgoode Hall Law School and the Collège d'Europe. He was a Canada-US Fulbright Scholar and earned his doctorate at Harvard Law School.

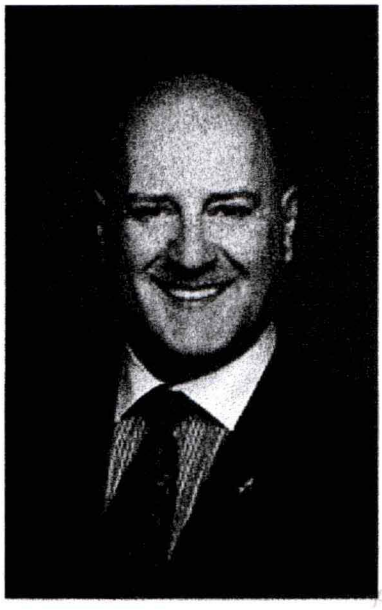
His professional experience spans the private sector, academia, government and international affairs. He served as a senior with the United Nations Assistance Mission for Iraq, where he led a team of experts to assist the Iraqi Parliament and Government of Iraq with political, constitutional and legal reforms. Mr. Spengemann also worked for a major Canadian bank and in the Privy Council Office in Ottawa. He held affiliations at the Munk School of Global Affairs, the Balsillie School of International Affairs and the Glendon School of Public & International Affairs.

Mr. Spengemann is also a member of the Standing Committee on National Defence (NDDN).

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada



Name: **Michel Picard**
Riding: **Montarville, Quebec**

Parliamentary Experience:

- First-Time MP

Activities/Experience of Interest to the Portfolio:

- Former Parliamentary Secretary to Minister of Public Safety
- Expert in financial crime

Michel Picard is an expert in financial crime and is the author of several articles and books on the subject. He has worked for a number of employers in both the private and public sectors, most notably for the Royal Canadian Mounted Police Integrated Market Enforcement Team, on its investigation of the Norbourg file. Michel also created and directed a Master's level course on combating financial crime within the Faculty of Management at the University of Sherbrooke's Longueuil campus.

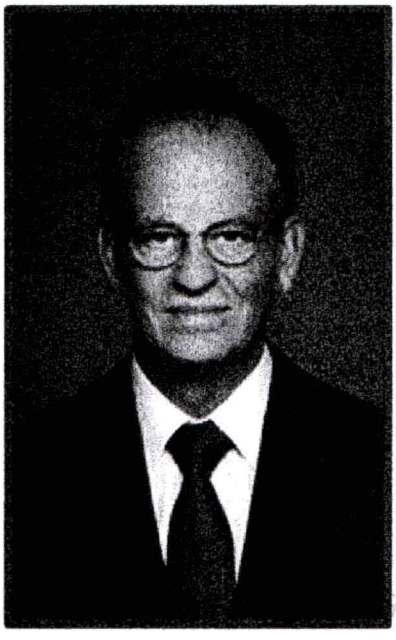
An international public speaker, Mr. Picard's expertise in the area of economic crime is much valued by Quebec's media. In this capacity, he is a guest analyst with RDI Matin Week end, where he comments on the testimonies heard at the Charbonneau Commission.

Mr. Picard holds both a Master's degree and a Doctorate in Political Science from l'Université de Paris X and a graduate diploma in Management from l'Université Laval.

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada



Name: Nicola Di Iorio
Riding: Saint-Léonard — Saint-Michel, Quebec

Parliamentary Experience:
- First-Time MP

Activities/Experience of Interest to the Portfolio:
- Member of SECU (February 2016 - Present)
- Member of REGS
- Member's Statement February 3, 2016: support for "Avis de recherche" television channel, which supports police forces by dedicating to the search for suspects and people who have disappeared, as well as crime prevention.

A lawyer specializing in labour and employment law, Nicola Di Iorio is a partner at the national firm Langlois Kronström Desjardins. He has gained both recognition and respect through his 32 years of practice, repeatedly ranking among lawyers most frequently recommended by their peers in the annual survey by Lexpert Magazine. Mr. Di Iorio was also recognized as one of Canada's leading labour and employment law experts in the 2014 edition of The Best Lawyers in Canada. A well-known guest speaker, he teaches at McGill University and the professional training school of the Barreau du Québec.

Nicola Di Iorio co-founded Cool Taxi – a prepaid taxi coupon initiative that provides people with a safe way home. The initiative earned him a nomination for the 2015 Person of the Year award of the Chamber of Commerce and Industry of Saint-Laurent–Mount Royal. He is the Secretary of the Board of Centro Leonardo da Vinci – an organization that he co-founded – and Secretary of the Board of the Italian-Canadian Community Foundation of Quebec.

Nicola Di Iorio holds an LLB from Université de Sherbrooke and an LLM from Columbia University and has co-authored two works entitled Les normes du travail.

Mr. Di Iorio is also a member of the Standing Joint Committee for the Scrutiny of Regulations (REGS).

Updated February 2017

House of Commons Standing Committee on
Public Safety and National Security (SECU)

● Liberal Party of Canada

Name: **Pam Damoff**
Riding: **Oakville North – Burlington, ON**

Parliamentary Experience:

- First-Time MP

Activities/Experience of Interest to the Portfolio:

- Member of SECU (February 2016 - Present)
- Interested in women's issues

Pam Damoff is a business professional and community activist who has served as a town councillor in Oakville since 2010.

On February 4, 2016, Ms. Damoff made a Statement for Members in the House of Commons in support for Brock University's "Women in the House" program, which seeks to better acknowledge and increase female participation in all levels of government.

Ms. Damoff was the proud recipient of the Queen Elizabeth II Diamond Jubilee medal and Paul Harris Fellow Award for her community service and the Top 40 Fabulous Women Over 40 Excellence Award for Community Leadership.

She earned a Bachelor of Arts degree from the University of Western Ontario.

Ms. Damoff is the first Vice-Chair of the Standing Committee on the Status of Women (FEWO).

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Conservative Party of Canada

FIRST VICE-CHAIR

Name: **Larry Miller**
Riding: Bruce-Grey-Owen Sound, Ontario

Parliamentary Experience:

- MP since 2004

Activities/Experience of Interest to the Portfolio:

- Member of SECU (January 2016 - Present)
- Deputy Critic for Public Safety and Emergency Preparedness

Larry Miller has been the Member of Parliament for Bruce-Grey-Owen Sound for four consecutive terms. Prior to entering federal politics, Mr. Miller worked in the farming industry and spent 13 years in municipal politics.

Mr. Miller has served on a number of House of Commons Committees. He sat as a Government Representative on the Standing Committee on Agriculture and Agri-Food from 2004-2012 and was Chair of this committee from 2008 to September of 2012. He was also a member of the Standing Committee on International Trade from 2006-2008. He was also Chair of the Standing Committee on Transport Infrastructure and Communities.

Larry Miller has sponsored Bill S-215: *An Act to Protect Heritage Lighthouses*, which received Royal Assent on May 29, 2008. He has also successfully passed a Private Members' Bill, Bill C-383: *The Transboundary Waters Protection Act*, which received Royal Assent on June 19, 2013.

On February 16, 2016, Mr. Miller introduced Bill C-230, *An Act to amend the Criminal Code* (variant of a firearm), which seeks to amends the *Criminal Code* to provide a definition of "variant" in order to limit its application to certain firearms. This was defeated on October 19, 2016.

He is currently the Conservative Party Deputy Critic for Public Safety and Emergency Preparedness.

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Conservative Party of Canada

Name: **Hon. Tony Celement**

Riding: Parry Sound – Muskoka, Ontario

Parliamentary Experience:

- MP since 2006
- Currently the Public Safety Critic

Activities/Experience of Interest to the Portfolio:

- Member of SECU (September 2016 - Present)

During his private sector career, Mr. Clement has been a lawyer, a business board member and a small business owner and entrepreneur.

Since his election to the House of Commons, Mr. Clement has served as Treasury Board President, Minister of Health and Minister of Industry. Within the federal government, he has also chaired five different Committees of Cabinet and served on the Priorities and Planning Committee, chaired by the Prime Minister.

A graduate of the University of Toronto, Mr. Clement completed degrees in political science in 1983 and law in 1986.

He was most recently the Conservative Party's Official Opposition Critic for Foreign Affairs but stepped down to launch his campaign for the leadership of the Conservative Party. He ended his campaign on October 12, 2016. He is currently the Public Safety Critic.

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

Conservative Party of Canada

Name: **Dianne L. Watts**
Riding: South Surrey-White Rock, BC

Parliamentary Experience:

- First-Time MP

Activities/Experience of Interest to the Portfolio:

- Infrastructure and Communities Critic
- Urban Affairs Critic

Ms. Watts has long been a leader in her local South Surrey – White Rock community, with a dedication to public service spanning nearly two decades. From 2005-2014, Ms. Watts served three terms as the first female Mayor of Surrey, and served a previous three terms as a Surrey City Councillor from 1996-2005.

Ms. Watts has led a diverse private sector career. Her experience includes consulting for and co-managing an architecture firm, and serving as CEO of a non-profit that supports and assists start-up companies commercialize technology.

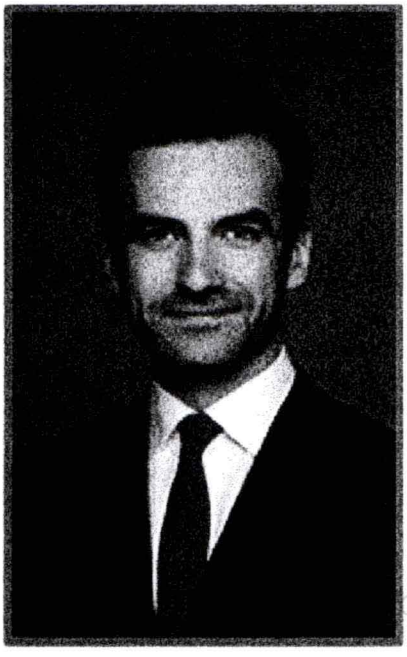
She has received international recognition as the 4th best mayor in the world by the City Mayor's Foundation in the UK in 2010 and is a recipient of the 2012 Queen Elizabeth II Diamond Jubilee Medal to honour her significant contributions to and achievements for her community.

She is currently the Infrastructure and Communities Critic, as well as the Urban Affairs Critic.

Updated February 2017

House of Commons Standing Committee on Public Safety and National Security (SECU)

New Democratic Party of Canada



SECOND VICE-CHAIR

Name: **Matthew Dubé**
Riding: **Beloeil – Chambly, Quebec**

Parliamentary Experience:

- MP Since 2011

Activities/Experience of Interest to the Portfolio:

- Deputy NDP House Leader
- Critic for Public Safety and Emergency Preparedness
- Critic for Infrastructure and Communities

As Member of Parliament since May 2011, Matthew Dubé has served as the NDP critic for Sports and Youth. He is currently the Critic for Public Safety and Emergency Preparedness, as well as for Infrastructure and Communities.

In the previous Parliament, Mr. Dubé was sitting on the Standing Committee on Public Accounts and Standing Committee on Canadian Heritage.

Mr. Dubé obtained his Bachelor of Arts degree in Political Science and History from McGill University.

Updated February 2017